PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-176551
(43)Date of publication of application : 21.06.2002

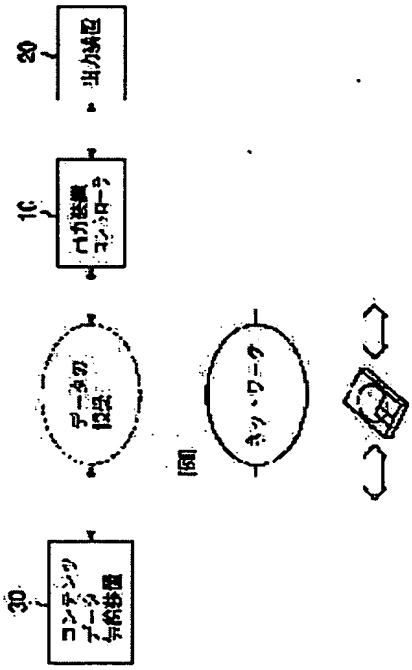
(51)Int.Cl. H04N 1/387
B41J 21/00
B41J 29/00
G06T 1/00
H04N 5/76
H04N 7/173

(21)Application number : 2000-372330
(22)Date of filing : 07.12.2000

(71)Applicant : NEC CORP
(72)Inventor : MANABE KOJI

(54) METHOD AND DEVICE FOR CONTENTS DATA SUPPLY, AND OUTPUT DEVICE CONTROLLER

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a technique for properly protecting copyright of contents and to provide a device and a system for implementing this technique.
SOLUTION: When supplying contents data, a contents data supply device 30 obtains an ID of an output device 20 which a user who desires this contents data has, from the user and embeds electronic watermark information including this ID in contents data and specifies an output device 20 capable of output to deliver contents data. An output device controller 10 acquires the ID of the output device 20 from the output device 20 and reports it to the contents data supply device 30 and uses this ID to discriminate the title to handing of data received from the contents data supply device 30 and deforms data in accordance with the title and transmits deformed data to the output device and thus mediates data.



LEGAL STATUS

[Date of request for examination] 28.11.2001
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number] 3596604
[Date of registration] 17.09.2004
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of

rejection]

[Date of extinction of right]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]
[Claim 1] The 1st step which stores the original contents data concerning original contents, The 2nd step to which the input of ID of the output unit which the user concerned owns is urged to the user who wishes supply of original contents data, The digital-watermarking information which contains in a part said ID inputted by the user according to the predetermined digital-watermarking approach [handling / an approach] by the output unit controller which said user owns is inserted in said original contents data. The contents data supply approach characterized by including the 3rd step which generates contents data with a mark, and the 4th step which supplies said contents data with a mark to said user.
[Claim 2] The digital-watermarking information inserted in said 3rd step is the contents data supply approach according to claim 1 characterized by being what forms a visible mark on said original contents.
[Claim 3] Said original contents data are the contents data supply approach according to claim 2 characterized by being image data.
[Claim 4] The contents data supply approach according to claim 1 characterized by supplying for a printer the data which can be printed as said original contents data as said output unit.
[Claim 5] Said 4th step is the contents data supply approach according to claim 1 characterized by being carried out by transmitting said contents data with a mark through a network to said user.
[Claim 6] Said 4th step is the contents data supply approach according to claim 1 characterized by being carried out by storing said contents data with a mark to the are recording medium which said user prepared.
[Claim 7] It is the contents data supply approach according to claim 1 which performs authentication processing using electronic signature among said users, is further equipped with the step which generates the common key shared with this user, and is characterized by said 4th step being what supplies said contents data with a mark enciphered with said common key.
[Claim 8] The contents data supply approach according to claim 1 characterized by having further the step which relates the use tariff of said original contents data with the original contents data concerned, and stores it beforehand, the step which acquires said use tariff related with the original contents data which said user wished to have, and the step which notifies the acquired use tariff concerned to said user.
[Claim 9] The storing section which stores the original contents data concerning original contents, ID acquisition section which acquires ID of the output unit which a user to the user concerned who wishes supply of original contents data owns, The digital-watermarking information which contains said acquired ID in a part according to the digital-watermarking approach [handling / an approach] by the output unit controller which said user owns is inserted in said original contents data. The contents data feeder characterized by including the digital-watermarking insertion section which generates contents data with a mark, and the feed zone which supplies said contents data with a mark to said user.
[Claim 10] The digital-watermarking information inserted in said digital-watermarking insertion section is a contents data feeder according to claim 9 characterized by forming a visible mark on said original contents.
[Claim 11] It is the contents data feeder according to claim 9 characterized by connecting said ID acquisition section and said feed zone to the network where the output unit controller which said user owns was connected, and performing acquisition of said ID, and supply of said contents data with a mark through said network.
[Claim 12] Reading of the information recorded on the record medium of the 1st class is possible for said ID acquisition section. Acquisition of said ID It is carried out by reading said ID from said 1st kind of record medium which said user by whom said ID was stored beforehand owns. Said feed zone Information can be written in to the record medium of the 2nd class. Supply of said contents data with a mark The contents data feeder according to claim 9 characterized by being carried out by writing in said contents data with a mark to said 2nd kind of record medium which said user owns.
[Claim 13] [when it is what has the 1st authentication section for performing an electronic authentication / said output unit controller] this -- authentication processing being performed between the 1st authentication section, and with the 2nd authentication section which generates the common key shared with said output unit controller Have further the encryption section which enciphers said contents data with a mark generated in said digital-watermarking insertion section using said common key generated in the 2nd authentication section, and said feed zone receives said user. this -- The contents data feeder according to claim 9 characterized by supplying said enciphered contents data with a mark.
[Claim 14] Said storing section is a contents data feeder according to claim 9 characterized by to have further the accounting-information Management Department which notifies the use tariff which associates and stores the use tariff of said original contents data in said original contents data, set in that case, acquired said use tariff related with the original contents data which said user wished to have from said storing section, and was acquired to said user.
[Claim 15] It is the output unit controller used in the condition of having connected with the output unit and the contents data feeder. Said output unit is what has ID of a proper. While said contents data feeder inserts ID of said output unit as a part of digital-watermarking information to original contents data according to the predetermined digital-watermarking approach In the output unit controller which is what outputs the original contents data with which said digital-watermarking information was inserted as contents data with a mark While acquiring said ID from said output unit and notifying to said contents data feeder ID acquisition section holding the acquired ID concerned, and the contents acquisition section which acquires said contents data with a mark from said contents data feeder, The digital-watermarking extract section which extracts digital-watermarking information from the acquired contents data with a mark, ID judging section which

compares ID currently held in the part and said ID acquisition section of the extracted digital-watermarking information, and judges whether both are the same, The contents data variant part which generates the contents data which deformed by transforming said contents data with a mark when both were the same as a result of the judgment in this ID judging section, The output unit controller characterized by having the output-data generation section which generates the output data [handling / output data] in said output unit from said contents data which deformed.
[Claim 16] The deformation in said contents data variant part is an output unit controller according to claim 15 characterized by what is been removing said digital-watermarking information from said contents data with a mark, and restoring said original contents data.
[Claim 17] [while having the 1st authentication section for performing an electronic authentication / said contents data feeder /, when it is what can encipher said contents data with a mark with a predetermined key] this -- authentication processing being performed between the 1st authentication section, and with the 2nd authentication section which generates the common key shared with said contents data feeder as said predetermined key From said contents data with a mark enciphered using said common key in said contents data feeder The output unit controller according to claim 15 which decrypts said contents data with a mark and is characterized by having further the decode section which outputs said decrypted contents data with a mark to said contents acquisition section.
[Claim 18] It is the output unit controller used in the condition of having connected with the output unit and the contents data feeder. Said output unit is what has ID of a proper. While said contents data feeder inserts the 1st digital-watermarking information which contains ID of said output unit in a part to original contents data according to the predetermined digital-watermarking approach In the output unit controller which is what outputs the original contents data with which the 1st digital-watermarking information was inserted as 1st contents data with a mark this -- While acquiring said ID from said output unit and notifying to said contents data feeder ID acquisition section which holds the acquired ID concerned temporarily, and the contents acquisition section which acquires said 1st contents data with a mark from said contents data feeder, it acquired -- this -- with the digital-watermarking extract section which extracts the 1st digital-watermarking information from the 1st contents data with a mark ID judging section which compares ID contained in a part of 1st extracted digital-watermarking information with ID currently held in said ID acquisition section, and judges whether both are the same, The contents data variant part which generates the contents data which deformed by transforming said 1st contents data with a mark when both were the same as a result of the judgment in this ID judging section, The controller side digital-watermarking insertion section which inserts a part of 2nd digital-watermarking information which contains ID currently held in said ID acquisition section to said contents data which deformed in a part, and generates the 2nd contents data with a mark, this -- the output unit controller characterized by having the output-data generation section which generates the output data [handling / output data] in said output unit from the 2nd contents data with a mark.

[Claim 19] The 2nd digital-watermarking information inserted in said controller side digital-watermarking insertion section is an output unit controller according to claim 18 characterized by being what forms an un-visible mark on the contents which said contents data which were generated in said contents data variant part, and which deformed show.
[Claim 20] The deformation in said contents data variant part is an output unit controller according to claim 18 characterized by what is been removing said digital-watermarking information from said contents data with a mark, and restoring said original contents data.
[Claim 21] [while having the 1st authentication section for performing an electronic authentication / said contents data feeder /, when it is what can encipher said contents data with a mark with a predetermined key] this -- authentication processing being performed between the 1st authentication section, and with the 2nd authentication section which generates the common key shared with said contents data feeder as said predetermined key From said contents data with a mark enciphered using said common key in said contents data feeder The output unit controller according to claim 18 which decrypts said contents data with a mark and is characterized by having further the decode section which outputs said decrypted contents data with a mark to said contents acquisition section.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention] Especially this invention relates to a system about the handling of a digital content at the equipment list which embodies the handling and it of a digital content concerning the protection of copyrights of contents.
[0002]
[Description of the Prior Art] Conventionally, the approach of protecting the copyright of contents to the print-line sake using a printer is proposed variously.
[0003] As a means to embody this kind of approach, and it, what is indicated by JP,2000-165652,A (henceforth "the related technique 1") and JP,2000-194832,A (henceforth "the related technique 2") is mentioned, for example.
[0004] The related technique 1 makes it a technical problem to control print data appropriately and to protect the copyright of a digital content, when printing the digital content where digital watermarking is embedded by the printer. As a technique for solving this technical problem, the related technique 1 extracted digital watermarking, embedded it at the concentration value of an image, performed modification processing of adding information and has proposed the technique which transforms an image.
[0005] In case the related technique 2 saves objects, such as a graphic form and an alphabetic character, as data, when the additional information acquired from a user at the time of the output of data differs from the additional information already embedded, it has proposed the technique which prevents from outputting data by embedding additional information by digital watermarking to the data.
[0006] Moreover, as other techniques using the technique of digital watermarking relevant to this invention, JP,11-239129,A (henceforth "the related technique 3"), JP,2000-227756,A (henceforth "the related technique 4"), and JP,2000-227757,A (henceforth "the related technique 5") are mentioned. These relation technique 3 thru/or 5 have higher dependability, and enables authentication of the relation between "electronic data, and an individual/engine, Moreover, showing [a user / directly]-with electronic data-individual/engine with which it has relation with electronic data that it is in agreement with individual/engine which can attest relation, electronic data, so that it may be guaranteed" is made into a technical problem. Using a purchaser's public key as the The means for solving a technical problem, "provider equipment enciphers the contents which the purchaser purchased and is sent. Purchaser equipment embeds the electronic signature which created and created the electronic signature of contents using the own private key to the contents to which it was sent as digital watermarking. When an illegal copy comes to hand, provider equipment verifies the electronic signature of digital watermarking, and proposes" technique of specifying the purchaser who purchased the contents which became the origin of this illegal copy.
[0007] Furthermore, what is indicated by JP,11-119651,A (henceforth "the related technique 6") is mentioned as other techniques relevant to this invention. In this related technique 6, in case a visible mark is eliminated and an un-visible mark is embedded, the technique of performing elimination of a visible mark and embedding of an un-visible mark for making indivisible elimination of a visible mark and embedding of an un-visible mark in parallel as a technical problem is shown.
[0008]
[Problem(s) to be Solved by the Invention] However, by technique which is looked at by the related technique mentioned above, the protection of copyrights of contents may not be made appropriately.
[0009] For example, in the related technique mentioned above, when the most, digital watermarking inserted in contents is the information and user ID which the user inputted, and a user can treat it direct picking. Therefore, this user is able to inform a third person of those information and ID with malice, and the third person who acquired those information etc. may be able to perform unjust use of contents. That is, the effectiveness which eliminates unjust use of contents only with the related technique mentioned above is thin.
[0010] Then, this invention aims at offering the equipment which embodies the technique and it which can plan the protection of copyrights of contents more appropriately after being based on the related technique mentioned above, and a system.
[0011]
[Means for Solving the Problem] The artificer of this invention paid his attention to the property with a digital content, as a result of repeating examination, in order to solve the technical problem mentioned above.
[0012] That is, since a stereo is data while it has the description that a thing homogeneous as original can be reproduced, human being can recognize a digital content only after it is outputted to a certain output unit.
[0013] Moreover, in the gestalt of unjust use of contents, transfer of contents data poses a problem from transfer of the very thing, such as an image printed, for example, so that clearly also from the description of the digital content "a thing homogeneous as original can be reproduced" described previously. And in such a case, those who handed contents data unjustly, and those who received it unjustly are separately considered to own the output unit for outputting the contents data concerned, respectively. In addition, if there is an output unit here when for example, contents data are image data, it is a printer etc., and if it is in other data, it points out the equipment which can deal with the data.
[0014] I acquired ID of the output unit which a user to the user concerned who asks for it when the artificer of this invention supplies contents data from these things owns, and thought it effective to build the system of distributing contents data where the output unit in which an output is possible is specified as embedding digital-watermarking information which contains the ID to contents data.
[0015] In such a system, when the case where contents data are image data, for example, and an output unit is a printer is taken for an example, the image shown by the image data concerned only by the printer which the user who acquired image data to normal owns can be

printed. That is, even if it passes a third person image data unjustly, by the printer which the third person concerned has, a third person cannot print the image but can plan protection of copyrights appropriately rather than the related technique mentioned above. And such a concept can be applied also when an output unit is not a printer, and it is effective also about contents data other than image data.
[0016] Specifically, this invention offers the contents data supply approach shown below as The means for solving a technical problem mentioned above.
[0017] Namely, the 1st step which stores the original contents data concerning original contents according to this invention, The 2nd step to which the input of ID of the output unit which the user concerned owns is urged to the user who wishes supply of original contents data, The digital-watermarking information which contains in a part said ID inputted by the user according to the predetermined digital-watermarking approach [handling / an approach] by the output unit controller which said user owns is inserted in said original contents data. The contents data supply approach characterized by including the 3rd step which generates contents data with a mark, and the 4th step which supplies said contents data with a mark to said user is acquired.
[0018] It is good also as being what forms a visible mark for the digital-watermarking information inserted in said 3rd step on said original contents here.
[0019] Moreover, said original contents data are good also as being image data.
[0020] Furthermore, it is good also as supplying for a printer the data which can be printed as said original contents data as said output unit.

[0021] Moreover, by transmitting said contents data with a mark through a network to said user, said 4th step is good also as being carried out, and good also as being carried out by storing said contents data with a mark to the are recording medium which said user prepared.
[0022] Furthermore, the contents data supply approach mentioned above may be applied as follows.
[0023] That is, in the contents data supply approach mentioned above, authentication processing using electronic signature is performed among said users, it has further the step which generates the common key shared with this user, and said 4th step is good also as being what supplies said contents data with a mark enciphered with said common key.
[0024] Moreover, in the contents data supply approach mentioned above, it is good also as having further the step which relates the use tariff of said original contents data with the original contents data concerned, and stores it beforehand, the step which acquires said use tariff related with the original contents data which said user wished to have, and the step which notifies the acquired use tariff concerned to said user.
[0025] Moreover, this invention also offers the contents data feeder which realizes the above-mentioned contents data supply approach so that it may enumerate below.
[0026] Namely, the storing section which stores the original contents data concerning original contents according to this invention, ID acquisition section which acquires ID of the output unit which a user to the user concerned who wishes supply of original contents data owns, The digital-watermarking information which contains said acquired ID in a part according to the digital-watermarking approach [handling / an approach] by the output unit controller which said user owns is inserted in said original contents data. The contents data feeder characterized by including the digital-watermarking insertion section which generates contents data with a mark, and the feed zone which supplies said contents data with a mark to said user is obtained.
[0027] It is good also as being what forms a visible mark for the digital-watermarking information inserted in said digital-watermarking insertion section on said original contents here.
[0028] Moreover, said ID acquisition section and said feed zone are connected to the network where the output unit controller which said user owns was connected, and it is good also as acquisition of said ID and supply of said contents data with a mark being performed through said network.
[0029] Reading of the information recorded on the record medium of the 1st class is possible for said ID acquisition section. Furthermore, acquisition of said ID It is carried out by reading said ID from said 1st kind of record medium which said user by whom said ID was stored beforehand owns. Said feed zone Information can be written in to the record medium of the 2nd class, and supply of said contents data with a mark is good also as being carried out by writing in said contents data with a mark to said 2nd kind of record medium which said user owns.
[0030] Furthermore, deformation may be added as follows to the contents data feeder mentioned above.
[0031] Namely, when it is what has the 1st authentication section for performing an electronic authentication [said output unit controller] in the contents data feeder mentioned above this -- authentication processing being performed between the 1st authentication section, and with the 2nd authentication section which generates the common key shared with said output unit controller Have further the encryption section which enciphers said contents data with a mark generated in said digital-watermarking insertion section using said common key generated in the 2nd authentication section, and said feed zone receives said user. this -- It is good also as supplying said enciphered contents data with a mark.
[0032] Moreover, it is good also as having further the accounting-information Management Department which notifies the use tariff which said storing section relates the use tariff of said original contents data with said original contents data in the contents data feeder mentioned above, stores, set in that case, acquired said use tariff related with the original contents data which said user wished to have from said storing section, and was acquired to said user.
[0033] Furthermore, this invention also offers the output unit controller which can constitute the system by this invention with the above-mentioned contents data feeder.
[0034] Namely, according to this invention, it is the output unit controller used in the condition of having connected with the output unit and the contents data feeder, as 1st output unit controller. Said output unit is what has ID of a proper. While said contents data feeder inserts ID of said output unit as a part of digital-watermarking information to original contents data according to the predetermined digital-watermarking approach In the output unit controller which is what outputs the original contents data with which said digital-watermarking information was inserted as contents data with a mark While acquiring said ID from said output unit and notifying to said contents data feeder ID acquisition section holding the acquired ID concerned, and the contents acquisition section which acquires said contents data with a mark from said contents data feeder, The digital-watermarking extract section which extracts digital-watermarking information from the acquired contents data with a mark, ID judging section which compares ID currently held in the part and said ID acquisition section of the extracted digital-watermarking information, and judges whether both are the same, The contents data variant part which generates the contents data which deformed by transforming said contents data with a mark when both were the same as a result of the judgment in this ID judging section, The output unit controller characterized by having the output-data generation section which generates the output data

[handling / output data] in said output unit is obtained from said contents data which deformed.
[0035] Here, the deformation in said contents data variant part is good also as what is been removing said digital-watermarking information from said contents data with a mark, and restoring said original contents data.
[0036] Moreover, while having the 1st authentication section for performing an electronic authentication [said contents data feeder], when it is what can encipher said contents data with a mark with a predetermined key, it sets. this -- authentication processing being performed between the 1st authentication section, and with the 2nd authentication section which generates the common key shared with said contents data feeder as said predetermined key From said contents data with a mark enciphered using said common key in said contents data feeder Said contents data with a mark are decrypted and it is good also as having further the decode section which outputs said decrypted contents data with a mark to said contents acquisition section.
[0037] Furthermore, according to this invention, it is the output unit controller used in the condition of having connected with the output unit and the contents data feeder, as 2nd output unit controller. Said output unit is what has ID of a proper. While said contents data feeder inserts the 1st digital-watermarking information which contains ID of said output unit in a part to original contents data according to the predetermined digital-watermarking approach In the output unit controller which is what outputs the original contents data with which the 1st digital-watermarking information was inserted as 1st contents data with a mark this -- While acquiring said ID from said output unit and notifying to said contents data feeder ID acquisition section which holds the acquired ID concerned temporarily, and the contents acquisition section which acquires said 1st contents data with a mark from said contents data feeder, it acquired -- this -- with the digital-watermarking extract section which extracts the 1st digital-watermarking information from the 1st contents data with a mark ID judging section which compares ID contained in a part of 1st extracted digital-watermarking information with ID currently held in said ID acquisition section, and judges whether both are the same, The contents data variant part which generates the contents data which deformed by transforming said 1st contents data with a mark when both were the same as a result of the judgment in this ID judging section, The controller side digital-watermarking insertion section which inserts a part of 2nd digital-watermarking information which contains ID currently held in said ID acquisition section to said contents data which deformed in a part, and generates the 2nd contents data with a mark, this -- the output unit controller characterized by having the output-data generation section which generates the output data [handling / output data] in said output unit is obtained from the 2nd contents data with a mark.
[0038] Here, the 2nd digital-watermarking information inserted in said controller side digital-watermarking insertion section is good also as being what forms an un-visible mark on the contents which said contents data which were generated in said contents data variant part, and which deformed show.
[0039] Moreover, the deformation in said contents data variant part is good also as what is been removing said digital-watermarking information from said contents data with a mark, and restoring said original contents data.
[0040] Furthermore, while having the 1st authentication section for performing an electronic authentication [said contents data feeder], when it is what can encipher said contents data with a mark with a predetermined key, it sets. this -- authentication processing being performed between the 1st authentication section, and with the 2nd authentication section which generates the common key shared with said contents data feeder as said predetermined key From said contents data with a mark enciphered using said common key in said contents data feeder Said contents data with a mark are decrypted and it is good also as having further the decode section which outputs said decrypted contents data with a mark to said contents acquisition section.
[0041]
[Embodiment of the Invention] Hereafter, the contents data distribution system which embodied the contents data supply approach and it by the gestalt of operation of this invention is explained using a drawing.
[0042] (Gestalt of the 1st operation) The contents data distribution system by the gestalt of operation of the 1st of this invention is equipped with the output unit controller 10, the output unit 20, and the contents data feeder 30 as shown in an outline and drawing 1 . Among these, the output unit 20 has ID of a proper and is connected with the output unit controller 10. Moreover, the output unit controller 10 can deliver and receive data between the contents data 30.
[0043] Here, it supposes that it mentions later about the detail of each equipment while giving an example variously, and first, referring to drawing 2 , about those outlines, it combines with outline actuation explanation of a system, and reference is made. In addition, although explained taking the case of a printer (therefore, a reference mark 20 is given to a "printer" below.) as an output unit 20 below, it cannot be overemphasized that the concept of this invention can apply similarly to other output units.
[0044] As shown in drawing 2 , the output unit controller 10 acquires ID of a printer 20 to the printer 20 concerned, and notifies it to the contents data feeder 30 side. The contents data feeder 30 embeds digital-watermarking information which contains ID notified from the output unit controller 10 to the contents data (in order to distinguish from the contents data with which deformation etc. is carried out hereafter, it is called "original contents data".) which the user who owns a printer 20 and the output unit controller 10 wishes to have, and supplies it to the output unit controller 20 as contents data with a mark. When both are the same, after it judged whether the output unit controller 10 would have ID which makes a part of digital-watermarking information inserted in contents data with a mark, and same ID acquired from the printer 20, and transforming contents data with a mark, the print data which can be printed by the printer 20 are generated. These print data are outputted from the output unit controller 10 to a printer 20, and are printed in a printer 20. Especially, in the gestalt of this operation, a printer 20 conducts self-investigation and notifies it to the output unit controller 10 by making into printing result information whether to have completed the printing result normally.
[0045] If it carries out from a contents data feeder side by adopting such technique, contents data can be distributed where the printer which can print is specified. Moreover, since it cannot print normally by the printer which cannot print to normal, namely, a third person has in it only by the printer which corresponded even if it is going to give a third person unjust use of delivering the duplicate of contents data at a user side, for example, control of unjust use is achieved.
[0046] Here, the transmission line which connects an output unit 20 and the output unit controller 10 is for example, an IEEE1394 high-speed serial bus (IEEE Std 1394-1995, Standard for a High Performance Serial Bus) and Universal. Serial It can constitute from serial interface, such as Bus (USB), a parallel interface used in order to connect a printer with a personal computer (it abbreviates to "PC" below.) from the former.
[0047] Moreover, as shown in drawing 1 , as a data transfer means between the output unit controller 10 and the contents data feeder 30, the network represented by the Internet, an are recording medium, a broadcast medium, etc. are employable, for example. If it is when adopting a network as a data transfer means, there is also no limit about the physical level which constitutes the network. That is, the telephone line (analog subscriber line), ISDN and xDSL, a cable modem, an optical fiber, etc. may use what kind of communication media.

Moreover, also about an are recording medium, there is especially no limit and it may use any, such as FD, and MO, CD-ROM, DVD, a magnetic tape. Also about a broadcast medium, CS digital broadcasting, BS digital broadcasting, land-based digital broadcasting, etc. are variously employable according to a system configuration.

[0048] When a data transfer means is the Internet, the contents data feeder 30 can be constituted from a WWW server made to cooperate with a database etc., and the output unit controller 10 can be constituted as plug-in of the WWW browser which works on PC of a user side. In this case, the contents data feeder 30 can notify the data input demand of various information offers, ID request, etc. to a user side WWW browser with gestalten, such as a Web page.

[0049] Moreover, when a data transfer means is an are recording medium, the contents data feeder 30 can be constituted as a KIOSK terminal installed in a convenience store etc., and can constitute the output unit controller 10 as a program which operates on PC which a user owns. In this case, if it is, the outline of contents data supply serves as the following, for example. First, a user once performs the program which realizes an output unit controller on PC to which the printer 20 was connected, and where ID of a printer is stored in an are recording medium, he goes out to the location in which the contents data feeder 30 is installed. The panel for notifying the directions to a user etc. is prepared in the contents data feeder 30, and the insertion demand of an are recording medium which stored ID there is displayed. If a user inserts an are recording medium in the contents feeder 30 according to the demand and specifies contents data, as the contents data feeder 30 was mentioned above, it will perform digital-watermarking insertion, and will write contents data with a mark in an are recording medium. A user performs the output unit controller 10 again on PC, processes the contents data with a mark memorized by the are recording medium, and prints to a printer 20.

[0050] Furthermore, if it is when it constitutes the contents data feeder 30 as a KIOSK terminal installed in a convenience store etc., it is good also as preparing the part of others which put the equipment which stores original contents data on a pin center,large, and perform digital-watermarking insertion etc. in a KIOSK terminal. Furthermore, if it is in this case, the connection between a pin center,large and a KIOSK terminal is good also as using the existing network.

[0051] In addition, as for the data delivered and received between the data and the output unit controller 10 which are exchanged between the output unit controller 10 and a printer 20, and the contents data feeder 30, it is desirable to perform suitable encryption processing, respectively. For example, it is possible to apply a SSL technique, XHTML, etc. in relation to the latter, when especially a data transfer means is the Internet. Moreover, when the processing performed inside each equipment of the output unit controller 10, a printer 20, and the contents data feeder 30 is attained by the combination of a processor and a program, it is desirable to use the Tampa register ring technique and to difficulty-in-reading-ize a processing program by the user, in order to prevent knowing the contents of processing or being altered.

[0052] The output unit controller 10 hereafter applicable to the contents data distribution system mentioned above using drawing 3 thru/or drawing 6 , a printer 20, and the contents data feeder 30 are explained more to a detail.

[0053] Drawing 3 is the block diagram showing the configuration of the output unit controller 10 in the gestalt of this operation, and a printer 20.

[0054] If drawing 3 is referred to, the output unit controller 10 is equipped with the contents acquisition section 110, the digital-watermarking extract section 120, ID judging section 130, the contents variant part 140, ID acquisition section 150, and the print-data generation section 160. On the other hand, the printer 20 is equipped with the printing section 220 for printing ID storing section 210 for storing self ID, and print data. Among these, ID storing section 210 is not limited to a certain hardware, and can consist of IC cards, non-volatilized memory cards, etc. which contain magnetic-recording media, such as semiconductor memory, such as ROM and RAM, and a magneto-optic disk, and these.

[0055] In the illustrated output unit controller 10, ID acquisition section 150 is notified to the contents data feeder 30 while it acquires ID from ID storing section 210 of a printer 20 and holds the ID temporarily. The digital-watermarking information which contains in a part by this ID notified to the contents data feeder 30 side to original contents according to the predetermined digital-watermarking method can be inserted, and the output unit controller 10 can be supplied as contents data with a mark. The contents acquisition section 110 acquires contents data with a mark from the contents data feeder 30. The digital-watermarking extract section 120 extracts the digital-watermarking information currently embedded to contents data with a mark. ID judging section 130 compares ID currently held temporarily at ID acquisition section 150 with ID (ID embedded at the contents data feeder side) which makes a part of digital-watermarking information, and judges whether both are in agreement. The contents variant part 140 performs deformation processing of contents data with a mark, and outputs the contents data which deformed. The deformation processing in the gestalt of this operation here removes digital watermarking from contents data with a mark, when ID which serve as a candidate for a comparison in ID judging section 130 is in agreement, and suppose that it is it what restores original contents data. From the contents data (namely, restored original contents data) which deformed, the print-data generation section 160 generates the print data [handling / print data] by the printer 20, and outputs them to the printing section 220. Thereby, in a printer 20, the original contents shown by original contents data are printed.

[0056] The digital-watermarking method used in the gestalt of this operation here is explained. The digital-watermarking method used in the gestalt of this operation should just be equipped with the ability to perform [that digital-watermarking information can be extracted in the digital-watermarking extract section 120 as the description, and] deformation of removal of digital watermarking etc. in the contents variant part 140. therefore, not the thing limited to a certain specific digital-watermarking method but Nakazato and Matsui: "the proposal of the signature watermark method which displays copyright positively" and the Institute of Image Electronics Engineers of Japan -- a method as shown by volume [27th] No. 5 (1998) can be used. It is suitable to use the signing method by the Peano scan and the two approaches of digital watermarking by the formation of distributed secrecy of signature information for coincidence in this method. In the signing method by the Peano scan, it is the description to prepare the pseudo-random-number sequence used for a signature to a subject-copy image, and to take the exclusive OR of a original pixel and a pseudo-random-number sequence in order of the Peano scan. Moreover, frequency conversion, such as a fast Fourier transform, a discrete cosine transform, and wavelet transform, is performed for example, to original contents data as other digital-watermarking methods, and after spacing through a frequency domain and adding information, the method which performs reverse frequency conversion can be used. After, as for the block with which the Fourier transform was performed for every block, it spaced further, and information was embedded after original contents data added and diffused PN sequence in the digital-watermarking method by said fast Fourier transform as an example, an inverse Fourier transform is performed, the again same PN sequence is added and digital watermarking should just be embedded.

[0057] Moreover, if reference is made about the approach of extracting the digital-watermarking information currently embedded to contents data with a mark in the digital-watermarking extract section 120, the method of acquiring the information about the approach of

extracting digital-watermarking information through the Internet, when the data transfer means shown, for example in drawing 1 is the Internet etc., and extracting digital-watermarking information based on this information is suitable.
[0058] Furthermore, as mentioned above, in the gestalt of this operation, the contents variant part 140 removes digital watermarking from contents data with a mark as deformation processing of contents data with a mark, and it performs restoring original contents data. It supposes that it is the digital-watermarking information where the digital-watermarking information inserted in the contents data feeder 30 was more specifically embedded by the visible mark, i.e., the digital-watermarking method of a visible mold, about this, and it is suitable for the contents variant part 140 to suppose that this visible mark is eliminated.
[0059] Moreover, in the print-data generation section 160, it is suitable for the processing which generates the print data [handling / print data / the contents data which deformed to the printer 20] to use the art which develops the binary-ized data of binary-ized Perilla frutescens (L.) Britton var. crispa (Thunb.) Decne. for image data in band memory for example, using the error diffusion technique etc., and the art which develops in band memory by use image data as multiple-value data again, and makes this data binary per raster line.
[0060] Drawing 4 is the block diagram showing other examples of a configuration of output unit controller 10a in the gestalt of this operation.
[0061] If drawing 4 is referred to, output unit controller 10a is equipped with the contents acquisition section 110, the digital-watermarking extract section 120, ID judging section 130, the contents variant part 140, ID acquisition section 150, the print-data generation section 160, and the digital-watermarking insertion section 170. Among these, the contents acquisition section 110, the digital-watermarking extract section 120, ID judging section 130, the contents variant part 140, and ID acquisition section 150 operate like what is contained in the output unit controller 10 shown in drawing 3 . Moreover, the print-data generation section 160 operates like what is shown in drawing 3 except for the point that a processing object is not the output of the contents variant part 140 but the output of the digital-watermarking insertion section 170 so that clearly from drawing 4 . Therefore, about these, the same reference mark as the example mentioned above is attached.
[0062] This illustrated output unit controller 10a is the point further equipped with the digital-watermarking insertion section 170, and differs from the output unit controller 10 mentioned above. This digital-watermarking insertion section 170 is for embedding digital-watermarking information which contains in a part ID currently held at ID acquisition section 150 as opposed to the contents data which the contents variant part 140 outputs and which deformed. In detail, the digital-watermarking insertion section 170 is for inserting it to the contents data which deformed for print-line reasons, such as identification information of the user who prints, identification information of the output unit controller 10, or ID of a printer 20, using as digital watermarking information that an identification information [about a person or a printing control system] and/or print-line sake is performed, such as hour entries, such as a date and time of day.
[0063] Here, considering as an un-visible mark is suitable for the watermark information embedded in the digital-watermarking insertion section 170. Moreover, as for the watermark information embedded in the contents data feeder 30 in this case, considering as a visible mark is desirable. Furthermore, the method (JP,11-119651,A) which performs elimination of a visible mark and embedding of an un-visible mark in parallel to the time of eliminating a visible mark and embedding an un-visible mark as a digital-watermarking method can also be used.
[0064] When unjust use of contents data arises, even if it is by considering output unit controller 10a as such a configuration, for example, it will become easy to specify the user who participated in it.
[0065] If here explains again the actuation in output unit controller 10a, in the illustrated output unit controller 10, ID acquisition section 150 will be first notified to the contents data feeder 30 while it acquires ID from ID storing section 210 of a printer 20 and holds the ID temporarily. The digital-watermarking information which contains in a part by this ID notified to the contents data feeder 30 side to original contents according to the predetermined digital-watermarking method can be inserted, and the output unit controller 10 can be supplied as contents data with a mark. The contents acquisition section 110 acquires contents data with a mark from the contents data feeder 30. The digital-watermarking extract section 120 extracts the digital-watermarking information currently embedded to contents data with a mark. ID judging section 130 compares ID currently held temporarily at ID acquisition section 150 with ID (ID embedded at the contents data feeder side) which makes a part of digital-watermarking information, and judges whether both are in agreement. The contents variant part 140 performs deformation processing of contents data with a mark, and outputs the contents data which deformed. Here, as mentioned above, the deformation processing in the gestalt of this operation removes digital watermarking from contents data with a mark, and restores original contents data. The digital-watermarking insertion section 170 performs insertion processing of digital watermarking to contents data (namely, original contents data restored in the gestalt of this operation) after deformation processing was performed. The print-data generation section 160 generates the print data [handling / print data] by the printer 20 from the contents data with which digital watermarking was inserted in the digital-watermarking insertion section 170, and outputs them to the printing section 220. Here, when digital watermarking inserted in the digital-watermarking insertion section 170 is an un-visible mark, print data present the same printing result as the case where original contents are printed. In response to such print data, a printer 20 prints the original contents shown by original contents data.
[0066] Next, with reference to drawing 5 , the concrete configuration of the contents data feeder 30 is explained.
[0067] As shown in drawing 5 , the contents data feeder 30 is equipped with the contents storing section 310, the digital-watermarking insertion section 320, a feed zone 330, and ID acquisition section 340. The contents storing section 310 stores original contents data beforehand. ID acquisition section 340 acquires ID of a printer 20 from the output unit controller 10 through data transfer means, such as the Internet. ID acquisition section 340 receives to the output unit controller 10 by the side of a user, sends ID sending-out demand etc., and the input of ID is urged to it, and, specifically, it acquires ID to which sending out etc. has been carried out by that cause. Under the present circumstances, in advance of this, the assignment of original contents data considered as a request is received from the user side immediately after this ID sending-out demand. If ID is received from ID acquisition section 340, the digital-watermarking insertion section 320 will acquire the original contents data for which a user asks from the contents storing section 310, and will embed acquired ID as digital-watermarking information to the original contents data according to the predetermined digital-watermarking insertion approach. The predetermined digital-watermarking insertion approach used here should be just the same as that of the digital-watermarking method which depends on a digital-watermarking method which was mentioned above, and is used in the digital-watermarking extract section 120. Furthermore, the digital-watermarking insertion section 320 outputs the original contents data with which such digital-watermarking information was embedded to a feed zone 330 as contents data with a mark. A feed zone 330 supplies contents data with a mark to the output unit controller 10 through data transfer means, such as the Internet.
[0068] It connects with that network, and both sides acquire ID through a network, and ID acquisition section 340 and the feed zone 330 in this contents data feeder 30 supply contents data with a mark for them through a network, when data transfer means are networks, such as

the Internet. On the other hand, when a data transfer means is an are recording medium, ID acquisition section 340 reads ID stored in the are recording medium, and a feed zone 330 writes contents data with a mark in an are recording medium. Here, the are recording medium by which ID was stored, and the are recording medium by which contents data with a mark are written in may be the same media, and may be different media.

[0069] It is the case where it is installed in a convenience store etc. although an usable thing is as having already stated also with a KIOSK terminal use gestalt [a contents data feeder], and when used with a gestalt which is connected with a pin center,large in a network, deforming, as shown in drawing 6 is also possible.

[0070] That is, contents data feeder 30a shown in drawing 6 is equipped with the digital-watermarking insertion section 320, a feed zone 330, and ID acquisition section 340 among the contents data feeders 30 shown in drawing 5 . On the other hand, contents enclosure 310a is prepared in the pin center,large side connected to contents data feeder 30a in a network. Like the contents storing section 310 shown in drawing 5 , this contents enclosure 310a stores original contents data, and consists of databases.

[0071] (Gestalt of the 2nd operation) The contents data distribution system by the gestalt of operation of the 2nd of this invention is explained using drawing 7 thru/or drawing 9 .

[0072] In the gestalt of this operation the contents data feeder 30 As are shown in drawing 7 , and in addition to the configuration (refer to drawing 5) by the gestalt of the 1st operation mentioned above it has the authentication section 350, the decryption section 360, and the encryption section 370 and the output unit controller 10 is also shown in drawing 8 In addition to the configuration (refer to drawing 3) by the gestalt of the 1st operation mentioned above, it has the authentication section 180, the encryption section 182, and the decryption section 184.

[0073] The authentication section 350 in a contents data feeder and the authentication section 180 in an output unit controller perform the electronic authentication according to a predetermined communications protocol through data transfer means, such as the Internet. It is suitable for this electronic authentication to carry out with electronic signature and a key delivery method. It is possible to use various methods devised until now as an electronic signature method and a key delivery method, for example, an ellipse DSA (Digital Signature Algorithm) signature and ellipse DH (Diffie-Hellman) key delivery can be used. An ellipse DSA signature (henceforth EC-DSA) is described below. EC-DSA is ANSI. It is specified to X9.62 etc. and the contents consist of three phases, key generation, signature generation, and signature collating. In addition, although the procedure in each of these phases is explained below, in order to omit the overlapping publication, it replaces with a contents data feeder and an output unit controller, and abstracts and explains like Devices A and B. If it puts in another way, if there is when operating as a device A and operating as a sink side by the initiative, if there is the authentication section 350 by the side of a contents data feeder when performing an electronic authentication, it will operate as a device B. On the other hand, the same is said of an output unit controller.

[0074] First, the procedure of key generation is explained.

(1) Set to the EC-DSA key generation device A, and it is the :step 1. : The elliptic curve E constituted on ZP is chosen. Divide the number of the points on E (ZP) among the big prime factor n.

Step 2: Point P**E (ZP) of order n is chosen.

Step 3: Section Statically characteristic and the integer d which cannot be predicted are chosen out of [1, n-1].

Step 4: Q=dP is calculated.

Step 5: The public key of A sets the private key of (E, P, n, Q), and A to d.

[0075] Below, a signature generation procedure is explained.

(2) Encipher Message m as follows in the EC-DSA signature generation device A.

Step 1: Section Statically characteristic and the integer k which cannot be predicted are chosen out of [1, n-1].

Step 2: kP= (x1, y1) and r=x1 mod n is calculated. It is considered by conversion from a binary expression here that x1 is one integer. If it becomes r=0, it will return to step 1 (reasons of security.). It is code equality if it is r= 0. s=k -1 {h(m)+dr} mod n Since a private key d is not included.

Step 3: k-1 mod n It calculates.

Step 4: s=k -1 {h(m)+dr} mod n is calculated. h is a secure hash algorithm (SHA-1) here.

Step 5: If it becomes s=0, it will return to step 1 (;s-1 in which s-1 mod n does not exist if it becomes s=0 is step 2 of signature collating, and it is the need).

step 6: the signature of Message m -- an integer -- constructing (r, s) -- ** -- it carries out.

[0076] Then, the procedure of signature collating is explained.

(3) In order to collate the signature (r, s) of the device A in the EC-DSA signature collating m, Device B performs the following things.

Step 1: The true copy of the public key (E, P, n, Q) of A is obtained.

Step 2: r and s are the section. [1 n-1] It collates that it is an integer.

Step 3: w=s -1 mod n and h (m) are calculated.

Step 4: u1=h (m) w mod n and u2=rw mod n is calculated.

Step 5: u1P+u2Q= (x0, y0) and v=x0 mod n is calculated.

Step 6: A signature will be accepted if it becomes v=r.

[0077] Next, ellipse DH key delivery (henceforth EC-DH) is described. EC-DH is ANSI. It is specified to X9.63 etc. and the contents consist of two phases key generation and exchange, and key shared. First, the procedure of key generation and exchange is as follows.

[0078] (1) Set to EC-DH key generation and the exchange device A, and it is step 1. : Section Statically characteristic and the integer x which cannot be predicted are chosen out of [2, n-2].

Step 2: a=xP is calculated.

Step 3: Device A sends a to Device B.

It sets to Device B and is step 1. : Section Statically characteristic and the integer y which cannot be predicted are chosen out of [2, n-2].

Step 2: b=yP is calculated. Device B sends b to Device A.

[0079] Next, a key shared procedure is described below.

(2) EC-DH key share step 1: In Device A, KA=xb=xyP generates a common key.

Step 2: In Device B, KB=xa=xyP generates a common key.

Step 3: Since it is KA=KB, Device A and Device B share a key.

Authentication processing is performed by the above procedures.

[0080] Thus, if sharing of a common key is made, in each of a contents data feeder and an output unit controller, encryption and decryption processing will be performed using this common key, and supply of the contents data using that encryption and decryption processing will be performed. In addition, the method of a code and decode can be used by any methods proposed until now.
[0081] Hereafter, also with reference to drawing 9 , actuation and the function of each part are explained collectively. First, a printer 20 notifies ID of the self stored in ID storing section 210 to the output unit controller 10 (notice of ID). Electronic signature is created using the authentication section 180, and it transmits to the contents data feeder 30, and on the other hand, the output unit controller 10 creates electronic signature using the authentication section 350, and transmits the contents data feeder 30 to the output unit controller 10 (electronic signature).
[0082] As a result of this electronic authentication processing, as the output unit controller 10 and the contents data feeder 30 were mentioned above, a common key will be shared.
[0083] Then, the authentication section 180 notifies the common key obtained as a result of authentication processing to the encryption section 182 and the decryption section 184. On the other hand, the authentication section 350 notifies the common key obtained as a result of authentication processing to a contents data feeder side at the decryption section 360 and the encryption section 370.
[0084] If the encryption section 182 by the side of an output unit controller moreover receives ID from ID acquisition section 150, using the common key, encryption processing is performed and ID enciphered at the contents data feeder side is sent out (notice of encryption ID).
[0085] If enciphered ID is received, using a common key, the decryption section 360 by the side of a contents data feeder will perform decryption processing, and will notify decrypted ID to ID acquisition section 340. Then, it is the same as the gestalt of the 1st operation mentioned above until contents data with a mark are outputted from a feed zone 330.
[0086] If contents data with a mark are received from a feed zone 330, using a common key, the encryption section 370 by the side of a contents data feeder will perform encryption processing, and will supply the enciphered contents data with a mark to an output unit controller side (encryption contents supply).
[0087] If the contents data with a mark enciphered from the contents data feeder side are received, the decryption section 184 by the side of an output unit controller will perform decryption processing using the common key which received from the authentication section 180, and will output the decrypted contents data with a mark to the contents acquisition section 110. Then, a process until print data are outputted and it is printed in a printer 20 from the print-data generation section 160 is performed like the gestalt of the 1st operation mentioned above. Moreover, also in the gestalt of this operation, like the gestalt of the 1st operation, a printer 20 conducts self-investigation and notifies it to the output unit controller 10 by making into printing result information whether to have completed the printing result normally.
[0088] In addition, also in the gestalt of this operation, in order to prevent the contents of processing being known by the user, or being altered about the processing performed inside each equipment, it is desirable to use the Tampa register ring technique and to difficulty-in-reading-ize a processing program.
[0089] Although the configuration which was mentioned above and which the both sides of the contents data feeder 30 and the output unit controller 10 equip with the encryption section (370 and 182) and the decryption section (360 and 184) as the gestalt of the 2nd operation is shown in drawing 7 and drawing 8 was shown good also as a configuration which it supposes that the contents data feeder 30 is equipped with the decryption section 360, and it does not have the encryption section 370, and the output unit controller 10 is equipped with the encryption section 182 on the other hand, and is not equipped with the decryption section 184 -- carrying out -- the -- it is good also as reverse. Furthermore, it is also possible to constitute the authentication section and the decryption section also in preparation for a printer 20.
[0090] Moreover, although explained using the example which deformed so that it might have the authentication section, the encryption section, and the decryption section in the gestalt of operation mentioned above by using as the base the output unit controller 10 and the contents data feeder 30 which are shown in drawing 3 and drawing 5 If it is good also as the base and what is shown in drawing 4 if it says about an output unit controller is said about a contents data feeder, it is good also considering what is shown in drawing 6 as the base.
[0091] (Gestalt of the 3rd operation) The contents data distribution system by the gestalt of operation of the 3rd of this invention is explained using drawing 10 thru/or drawing 12 .
[0092] In addition to the configuration (refer to drawing 5) by the gestalt of the 1st operation mentioned above, the contents data feeder in the gestalt of this operation has the accounting information Management Department 380, as shown in drawing 10 . The accounting information Management Department 380 has the database which comes to store accounting information, such as a use tariff related with original contents data, and sends out the accounting information according to the original contents data read from the contents storing section 310 to an output unit controller side. Here, the database which comes to store accounting information may be formed separately from the accounting information Management Department 380, and may be built into the contents storing section 310. Moreover, in the illustrated example, although considered as the configuration which included the accounting information Management Department 380 in the contents data feeder, it is good also as preparing this separately from a contents data feeder. In that case, even if it is, about the database which comes to store accounting information, such as a use tariff, you may be included in the independent accounting information Management Department, and it may be prepared so that it may become independent in itself, and may be included in the contents storing section 310.
[0093] In addition, other components 310 shown in drawing 10 , i.e., the contents storing section, the digital-watermarking insertion section 320, a feed zone 320, and ID acquisition section 340 operate like the gestalt of the 1st operation mentioned above.
[0094] On the other hand, in addition to the configuration (refer to drawing 3) by the gestalt of the 1st operation mentioned above, the output unit controller in the gestalt of this operation is equipped with the accounting information acquisition section 190, the charge calculation section 192 of accounting, and the electronic banking section 194 as shown in drawing 11 . The accounting information acquisition section 190 acquires accounting information from the accounting management storing section 380. Based on the accounting information which the accounting information acquisition section 190 acquired, for every predetermined period, the charge calculation section 192 of accounting totals accounting information, and computes the charge of accounting. The electronic banking section 440 is for settling electronically the accounting tariff which the charge calculation section 192 of accounting computed, and notifies settlement-of-accounts information to a contents data feeder (specifically accounting information Management Department). As the electronic banking technique in the electronic banking section 440, the existing electronic banking technique, such as a credit card and cybermoney, is employable. In addition, in drawing 11 , although considered as the configuration which included the accounting information acquisition

section 190, the charge calculation section 192 of accounting, and the electronic banking section 194 in the output unit controller, it is good also as preparing these separately from an output unit controller.
[0095] In addition, other components 110 shown in drawing 11 , i.e., the contents acquisition section, the digital-watermarking extract section 120, ID judging section 130, the contents variant part 140, ID acquisition section 150, and the print-data generation section 160 operate like the gestalt of the 1st operation mentioned above.
[0096] Hereafter, actuation of each part is explained also with reference to drawing 12 . First, a printer 20 notifies ID of the self stored in ID storing section 210 to the output unit controller 10 (notice of ID). The output unit controller 10 notifies this ID to the contents data feeder 30 further (notice of ID). The contents data feeder 30 embeds this ID to original contents data as a part of digital-watermarking information (digital-watermarking insertion), and supplies it to the output unit controller 10 as contents data with a mark (contents supply).
[0097] Especially, in the gestalt of this operation, the contents data feeder 30 (specifically accounting information Management Department) notifies the accounting information corresponding to the supplied contents data to the output unit controller 10 side according to the retrieval result of a database (notice of accounting information).
[0098] If contents data with a mark are received, the output unit controller 10 will perform ID judging, contents deformation, generation of print data, etc., and will output print data to a printer 20 (print-data output). The printing result which shows whether the printer 20 printed using print data and has been printed normally is notified to the output unit controller 10 (notice of a printing result).
[0099] In addition, in drawing 12 , although it is indicated that processing of ID judging in the output unit controller 10 etc. is performed after the notice of accounting information is performed, as for these processings, any may be performed first.
[0100] In an output unit controller, each processing of acquisition of accounting information, the total of the accounting information for every predetermined period, and electronic banking is performed by the accounting information acquisition section 190, the charge calculation section 192 of accounting, and the electronic banking section 194, and the accounting information Management Department 380 by the side of the contents data feeder 30 is notified of the settlement-of-accounts information finally acquired (notice of settlement-of-accounts information).
[0101] As for the information are delivered and received between each equipment like the gestalt of other above-mentioned operations also in the gestalt of this operation here, it is desirable to be performed suitable encryption processing, and in order to prevent the contents of processing being known by the user, or being altered about the processing to which it is carried out inside each equipment, it is desirable to use the Tampa register ring technique and to difficulty-in-reading-ize a processing program.
[0102] In addition, it sets in the gestalt of the 3rd operation mentioned above. Although explained using the example which deformed so that it might have the accounting information Management Department 380, the accounting information acquisition section 190, the charge calculation section 192 of accounting, and the electronic banking section 194 by using as the base the output unit controller 10 and the contents data feeder 30 which are shown in drawing 3 and drawing 5 If it is good also as the base and what is shown in drawing 4 if it says about an output unit controller is said about a contents data feeder, it is good also considering what is shown in drawing 6 as the base.
[0103]
[Effect of the Invention] As explained above, since contents data can be supplied where the output unit in which an output is possible is normally specified at the time of supply of contents data according to the contents data supply approach and system of this invention, the protection of copyrights of contents will make it more suitable.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1] It is drawing showing the outline configuration of the contents data distribution system by the gestalt of operation of this invention.
[Drawing 2] It is drawing showing outline actuation of the contents data distribution system by the gestalt of operation of the 1st of this invention.
[Drawing 3] It is drawing showing an example of an output unit controller applicable to the contents data distribution system by the gestalt of operation of the 1st of this invention, and a printer.
[Drawing 4] It is drawing showing other examples of an output unit controller applicable to the contents data distribution system by the gestalt of operation of the 1st of this invention, and a printer.
[Drawing 5] It is drawing showing an example of a contents data feeder applicable to the contents data distribution system by the gestalt of operation of the 1st of this invention.
[Drawing 6] It is drawing showing other examples of a contents data feeder applicable to the contents data distribution system by the gestalt of operation of the 1st of this invention.
[Drawing 7] It is drawing showing an example of an output unit controller applicable to the contents data distribution system by the gestalt of operation of the 2nd of this invention.
[Drawing 8] It is drawing showing an example of a contents data feeder applicable to the contents data distribution system by the gestalt of operation of the 2nd of this invention.
[Drawing 9] It is drawing showing outline actuation of the contents data distribution system by the gestalt of operation of the 2nd of this invention.
[Drawing 10] It is drawing showing an example of a contents data feeder applicable to the contents data distribution system by the gestalt of operation of the 3rd of this invention.
[Drawing 11] It is drawing showing an example of an output unit controller applicable to the contents data distribution system by the gestalt of operation of the 3rd of this invention.
[Drawing 12] It is drawing showing outline actuation of the contents data distribution system by the gestalt of operation of the 3rd of this invention.
[Description of Notations]
10 Output Unit Controller
110 Contents Acquisition Section
120 Digital-Watermarking Extract Section
130 ID Judging Section
140 Contents Variant Part
150 ID Acquisition Section
160 Print-Data Generation Section
170 Digital-Watermarking Insertion Section
180 Authentication Section
182 Encryption Section
184 Decryption Section
190 Accounting Information Acquisition Section
192 Charge Calculation Section of Accounting
194 Electronic Banking Section
20 Output Unit (Printer)
210 ID Storing Section
220 Printing Section
30 Contents Data Feeder
310 Contents Storing Section
320 Digital-Watermarking Insertion Section
330 Feed Zone
340 ID Acquisition Section
350 Authentication Section
360 Decryption Section
370 Encryption Section
380 Accounting Information Management Department

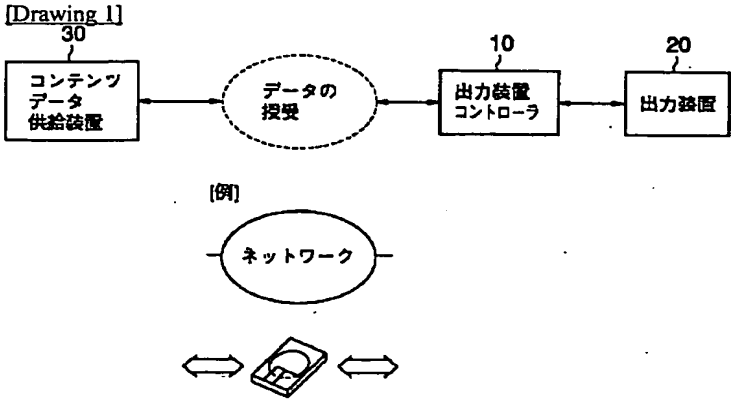
[Translation done.]

* NOTICES *

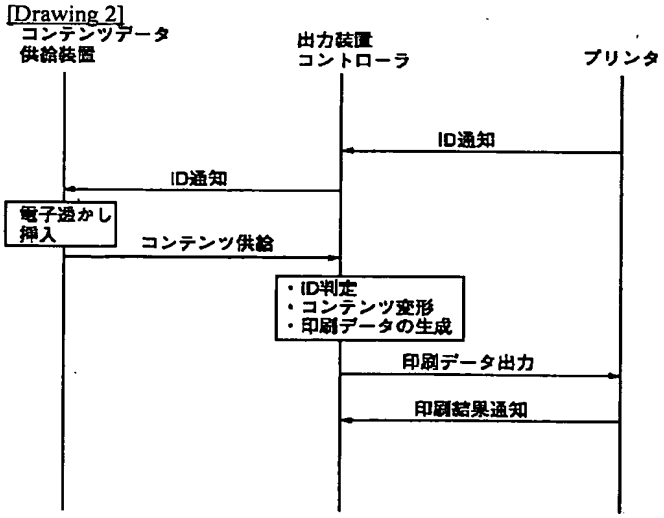
1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DRAWINGS

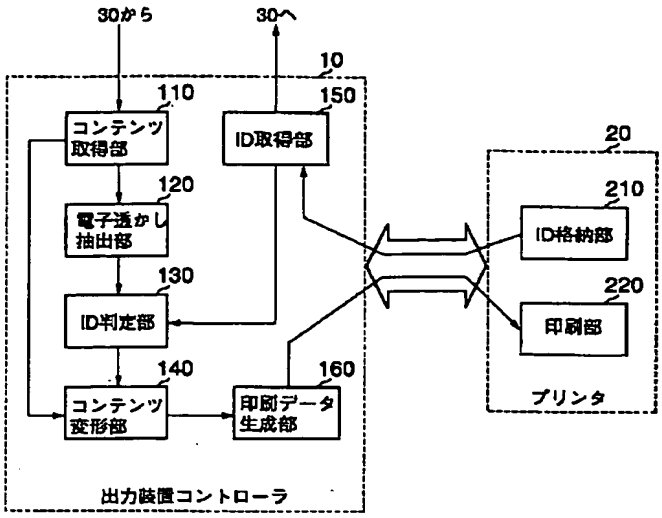
[Drawing 1]



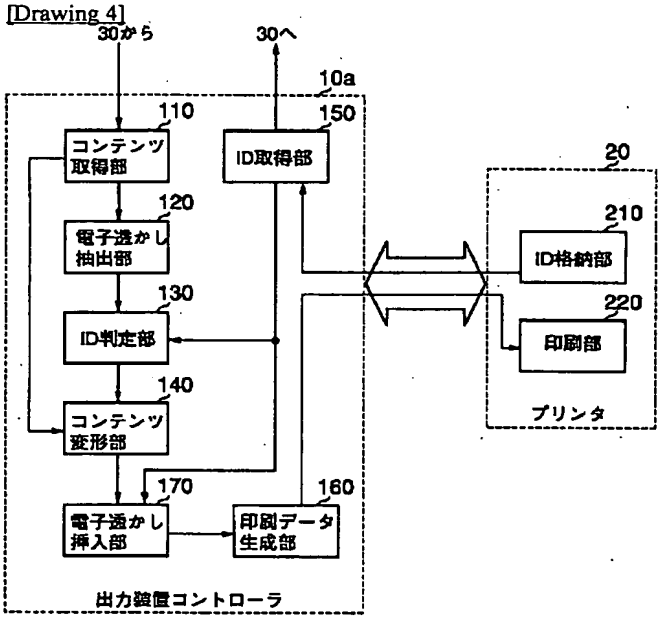
[Drawing 2]



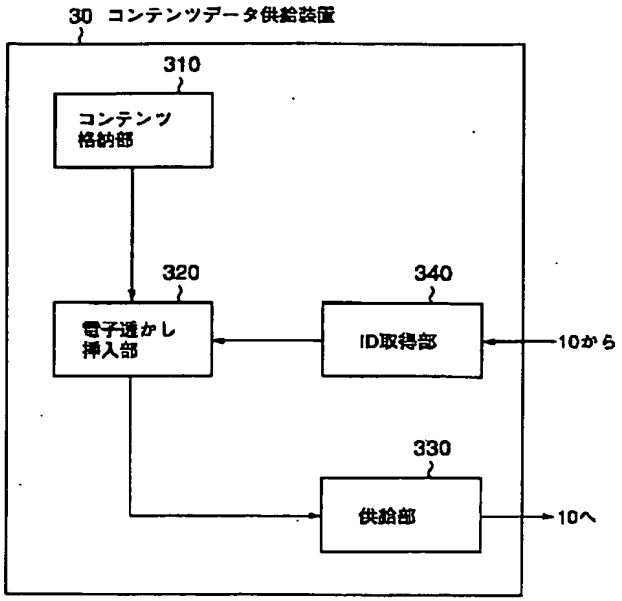
[Drawing 3]



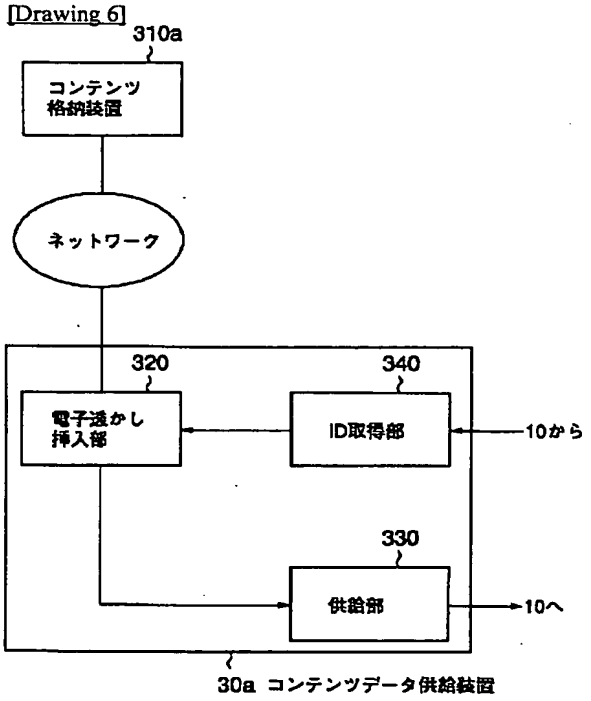
[Drawing 4]



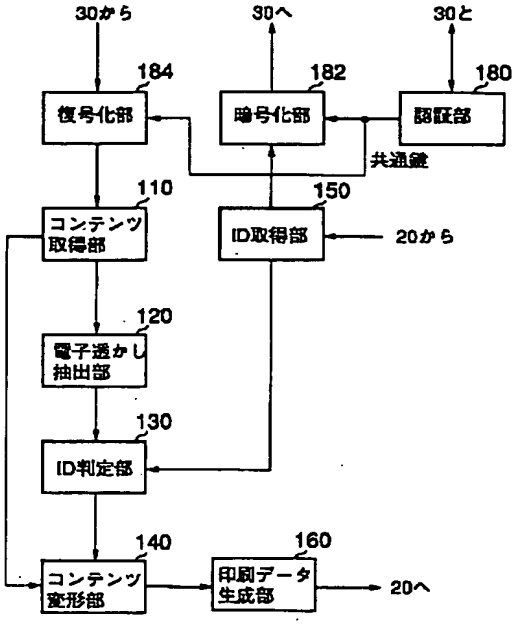
[Drawing 5]



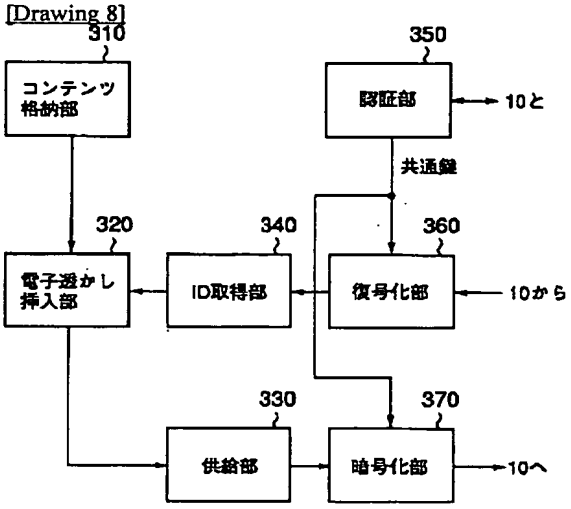
[Drawing 6]



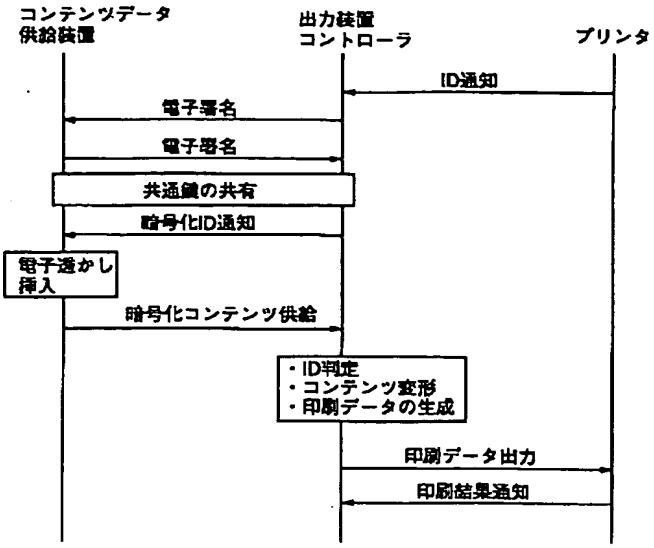
[Drawing 7]



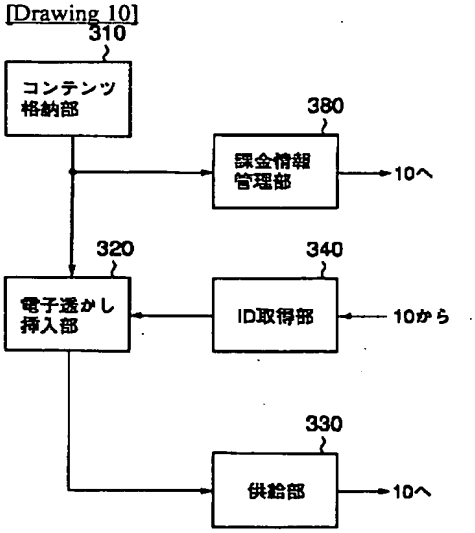
[Drawing 8]



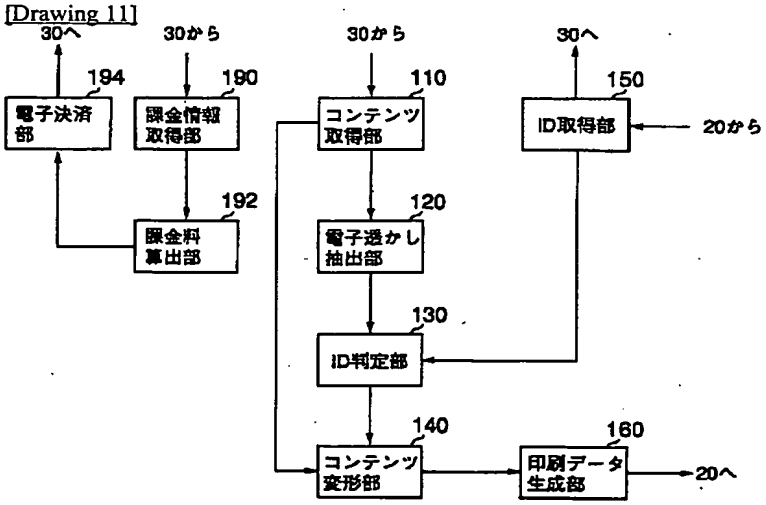
[Drawing 9]



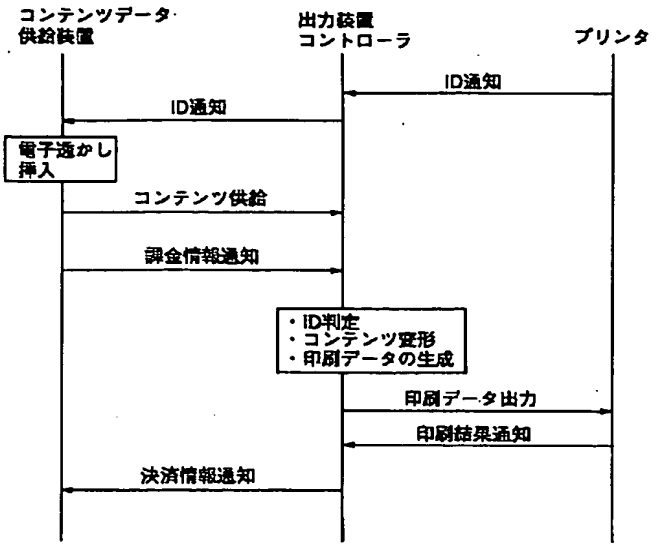
[Drawing 10]



[Drawing 11]



[Drawing 12]



[Translation done.]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－176551
（P2002－176551A）
(43)公開日　平成14年６月21日(2002.6.21)

(51)Int.Cl.'	識別記号	FI		テーマコード'（参考）
Ｈ０４Ｎ　1/387		Ｈ０４Ｎ　1/387		２Ｃ０６１
Ｂ４１Ｊ　21/00		Ｂ４１Ｊ　21/00	Ｚ	２Ｃ０８７
29/00		Ｇ０６Ｔ　1/00	５００Ｂ	２Ｃ１８７
Ｇ０６Ｔ　1/00	５００	Ｈ０４Ｎ　5/76	Ｅ	５Ｂ０５７
Ｈ０４Ｎ　5/76		7/173	６２０Ｄ	５Ｃ０５２

審査請求　有　請求項の数21　ＯＬ　（全 17 頁）　最終頁に続く

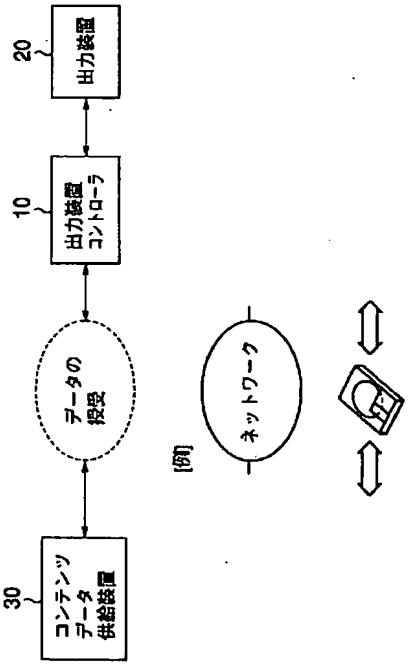
(21)出願番号　特願2000－372330(P2000－372330)
(22)出願日　平成12年12月７日(2000.12.7)

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号
(72)発明者　真鍋　浩嗣
東京都港区芝五丁目７番１号　日本電気株式会社内
(74)代理人　100071272
弁理士　後藤　洋介　（外１名）

最終頁に続く

(54)【発明の名称】　コンテンツデータ供給方法、コンテンツデータ供給装置、出力装置コントローラ

(57)【要約】
【課題】　適切にコンテンツの著作権保護を図ることのできる手法及びそれを具現化する装置やシステムを提供すること。
【解決手段】　コンテンツデータ供給装置３０は、コンテンツデータを供給するにあたって、それを所望するユーザから当該ユーザの所有する出力装置２０のＩＤを取得し、そのＩＤを含むような電子透かし情報をコンテンツデータに埋め込むこととして、出力可能な出力装置２０を特定した状態でコンテンツデータを配信する。出力装置コントローラ１０は、出力装置２０のＩＤを出力装置２０から取得して、コンテンツデータ供給装置３０に通知すると共に、そのＩＤを使って、コンテンツデータ供給装置３０から受けたデータの取り扱い権原を判断し、権原に応じたデータ変形を行って、変形されたデータを出力装置に伝えるという仲介を行う。



1

【特許請求の範囲】

【請求項１】　オリジナルコンテンツに係るオリジナルコンテンツデータを格納する第１のステップと、
オリジナルコンテンツデータの供給を希望するユーザに対して、当該ユーザの所有する出力装置のＩＤの入力を促す第２のステップと、
前記ユーザの所有する出力装置コントローラにより取り扱い可能な所定の電子透かし方法に従い、ユーザから入力された前記ＩＤを一部に含む電子透かし情報を前記オリジナルコンテンツデータに挿入して、マーク付コンテンツデータを生成する第３のステップと、
前記ユーザに対して、前記マーク付コンテンツデータを供給する第４のステップとを含むことを特徴とするコンテンツデータ供給方法。

【請求項２】　前記第３のステップにおいて挿入される電子透かし情報は、前記オリジナルコンテンツ上に可視マークを形成するものであることを特徴とする請求項１記載のコンテンツデータ供給方法。

【請求項３】　前記オリジナルコンテンツデータは、画像データであることを特徴とする請求項２記載のコンテンツデータ供給方法。

【請求項４】　前記出力装置としてプリンタを対象とし、前記オリジナルコンテンツデータとして印刷可能なデータを供給することを特徴とする請求項１記載のコンテンツデータ供給方法。

【請求項５】　前記第４のステップは、前記ユーザに対してネットワークを介して前記マーク付コンテンツデータを送信することにより、行われることを特徴とする請求項１記載のコンテンツデータ供給方法。

【請求項６】　前記第４のステップは、前記ユーザの用意した蓄積媒体に対して前記マーク付コンテンツデータを蓄積することにより、行われることを特徴とする請求項１記載のコンテンツデータ供給方法。

【請求項７】　前記ユーザとの間で電子署名を用いた認証処理を行い、該ユーザと共有する共通鍵を生成するステップを更に備え、
前記第４のステップは、前記共通鍵により暗号化された前記マーク付コンテンツデータを供給するものであることを特徴とする請求項１記載のコンテンツデータ供給方法。

【請求項８】　前記オリジナルコンテンツデータの利用料金を当該オリジナルコンテンツデータに関連付けて予め格納しておくステップと、
前記ユーザの希望したオリジナルコンテンツデータに関連付けられた前記利用料金を取得するステップと、
前記ユーザに対して当該取得した利用料金を通知するステップとを更に備えることを特徴とする請求項１記載のコンテンツデータ供給方法。

【請求項９】　オリジナルコンテンツに係るオリジナルコンテンツデータを格納する格納部と、

2

オリジナルコンテンツデータの供給を希望するユーザから当該ユーザの所有する出力装置のＩＤを取得するＩＤ取得部と、
前記ユーザの所有する出力装置コントローラにより取り扱い可能な電子透かし方法に従い、前記取得したＩＤを一部に含む電子透かし情報を前記オリジナルコンテンツデータに挿入して、マーク付コンテンツデータを生成する電子透かし挿入部と、
前記ユーザに対して、前記マーク付コンテンツデータを供給する供給部とを含むことを特徴とするコンテンツデータ供給装置。

【請求項１０】　前記電子透かし挿入部において挿入される電子透かし情報は、前記オリジナルコンテンツ上に可視マークを形成することを特徴とする請求項９記載のコンテンツデータ供給装置。

【請求項１１】　前記ＩＤ取得部及び前記供給部は、前記ユーザの所有する出力装置コントローラの接続されたネットワークに対して、接続されており、
前記ＩＤの取得及び前記マーク付コンテンツデータの供給は、前記ネットワークを介して行われることを特徴とする請求項９記載のコンテンツデータ供給装置。

【請求項１２】　前記ＩＤ取得部は、第１の種類の記録媒体に記録された情報を読取可能なものであり、前記ＩＤの取得は、予め前記ＩＤの格納された前記ユーザの所有する前記第１の種類の記録媒体から前記ＩＤを読み出すことにより行われ、
前記供給部は、第２の種類の記録媒体に対して情報を書込み可能なものであり、前記マーク付コンテンツデータの供給は、前記ユーザの所有する前記第２の種類の記録媒体に対して前記マーク付コンテンツデータを書込むことにより行われることを特徴とする請求項９記載のコンテンツデータ供給装置。

【請求項１３】　前記出力装置コントローラが電子認証を行うための第１の認証部を有するものである場合において、
該第１の認証部との間で認証処理を行い、前記出力装置コントローラと共有する共通鍵の生成を行う第２の認証部と、
該第２の認証部において生成された前記共通鍵を用いて、前記電子透かし挿入部において生成された前記マーク付コンテンツデータを暗号化する暗号化部とを更に備えており、
前記供給部は、前記ユーザに対して、暗号化された前記マーク付コンテンツデータを供給することを特徴とする請求項９記載のコンテンツデータ供給装置。

【請求項１４】　前記格納部は、前記オリジナルコンテンツデータの利用料金を前記オリジナルコンテンツデータに関連付けて格納するものであり、その場合において、
前記ユーザの希望したオリジナルコンテンツデータに関

連付けられた前記利用料金を前記格納部から取得し、前記ユーザに対して取得した利用料金の通知を行う課金情報管理部を更に備えることを特徴とする請求項９記載のコンテンツデータ供給装置。

【請求項１５】　出力装置とコンテンツデータ供給装置とに接続された状態で使用される出力装置コントローラであって、前記出力装置は固有のＩＤを有するものであり、前記コンテンツデータ供給装置は所定の電子透かし方法に従ってオリジナルコンテンツデータに対し前記出力装置のＩＤを電子透かし情報の一部として挿入すると共に前記電子透かし情報の挿入されたオリジナルコンテンツデータをマーク付コンテンツデータとして出力するものである、出力装置コントローラにおいて、

前記出力装置から前記ＩＤを取得し、前記コンテンツデータ供給装置に対して通知すると共に、当該取得したＩＤを保持するＩＤ取得部と、

前記コンテンツデータ供給装置から前記マーク付コンテンツデータを取得するコンテンツ取得部と、

取得したマーク付コンテンツデータから電子透かし情報を抽出する電子透かし抽出部と、

抽出した電子透かし情報の一部と、前記ＩＤ取得部において保持されていたＩＤとを比較し、両者が同一であるか否かを判定するＩＤ判定部と、

該ＩＤ判定部における判定の結果、両者が同一である場合に、前記マーク付コンテンツデータを変形して変形されたコンテンツデータを生成するコンテンツデータ変形部と、

前記変形されたコンテンツデータから、前記出力装置において取扱可能な出力データを生成する出力データ生成部とを備えることを特徴とする出力装置コントローラ。

【請求項１６】　前記コンテンツデータ変形部における変形は、前記マーク付コンテンツデータから前記電子透かし情報を除去して前記オリジナルコンテンツデータを復元することである、ことを特徴とする請求項１５記載の出力装置コントローラ。

【請求項１７】　前記コンテンツデータ供給装置が電子認証を行うための第１の認証部を有するものであると共に前記マーク付コンテンツデータを所定の鍵で暗号化することのできるものである場合において、

該第１の認証部との間で認証処理を行い、前記所定の鍵として、前記コンテンツデータ供給装置と共有する共通鍵の生成を行う第２の認証部と、

前記コンテンツデータ供給装置において前記共通鍵を用いて暗号化された前記マーク付コンテンツデータから、前記マーク付コンテンツデータを復号化し、復号化した前記マーク付コンテンツデータを前記コンテンツ取得部に出力する復号部とを更に備えることを特徴とする請求項１５に記載の出力装置コントローラ。

【請求項１８】　出力装置とコンテンツデータ供給装置とに接続された状態で使用される出力装置コントローラであって、前記出力装置は固有のＩＤを有するものであり、前記コンテンツデータ供給装置は所定の電子透かし方法に従ってオリジナルコンテンツデータに対し前記出力装置のＩＤを一部に含む第１の電子透かし情報を挿入すると共に該第１の電子透かし情報の挿入されたオリジナルコンテンツデータを第１のマーク付コンテンツデータとして出力するものである、出力装置コントローラにおいて、

前記出力装置から前記ＩＤを取得し、前記コンテンツデータ供給装置に対して通知すると共に、当該取得したＩＤを一時的に保持するＩＤ取得部と、

前記コンテンツデータ供給装置から前記第１のマーク付コンテンツデータを取得するコンテンツ取得部と、

取得した該第１のマーク付コンテンツデータから第１の電子透かし情報を抽出する電子透かし抽出部と、

抽出した第１の電子透かし情報の一部に含まれるＩＤと、前記ＩＤ取得部において保持されていたＩＤとを比較し、両者が同一であるか否かを判定するＩＤ判定部と、

該ＩＤ判定部における判定の結果、両者が同一である場合に、前記第１のマーク付コンテンツデータを変形して変形されたコンテンツデータを生成するコンテンツデータ変形部と、

前記変形されたコンテンツデータに対して前記ＩＤ取得部において保持されていたＩＤを一部に含む第２の電子透かし情報の一部を挿入し、第２のマーク付コンテンツデータを生成するコントローラ側電子透かし挿入部と、

該第２のマーク付コンテンツデータから、前記出力装置において取扱可能な出力データを生成する出力データ生成部とを備えることを特徴とする出力装置コントローラ。

【請求項１９】　前記コントローラ側電子透かし挿入部において挿入される第２の電子透かし情報は、前記コンテンツデータ変形部において生成された前記変形されたコンテンツデータの示すコンテンツ上に非可視マークを形成するものであることを特徴とする請求項１８記載の出力装置コントローラ。

【請求項２０】　前記コンテンツデータ変形部における変形は、前記マーク付コンテンツデータから前記電子透かし情報を除去して前記オリジナルコンテンツデータを復元することである、ことを特徴とする請求項１８記載の出力装置コントローラ。

【請求項２１】　前記コンテンツデータ供給装置が電子認証を行うための第１の認証部を有するものであると共に前記マーク付コンテンツデータを所定の鍵で暗号化することのできるものである場合において、

該第１の認証部との間で認証処理を行い、前記所定の鍵として、前記コンテンツデータ供給装置と共有する共通鍵の生成を行う第２の認証部と、

前記コンテンツデータ供給装置において前記共通鍵を用

いて暗号化された前記マーク付コンテンツデータから、前記マーク付コンテンツデータを復号化し、復号化した前記マーク付コンテンツデータを前記コンテンツ取得部に出力する復号部とを更に備えることを特徴とする請求項１８に記載の出力装置コントローラ。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、デジタルコンテンツの取り扱いに関し、特に、コンテンツの著作権保護に係るデジタルコンテンツの取り扱い及びそれを具現化する装置並びにシステムに関する。

【０００２】

【従来の技術】従来、プリンタを用いた印刷行為においてコンテンツの著作権を保護する方法が種々提案されている。

【０００３】この種の方法及びそれを具現化する手段としては、例えば、特開２０００－１６５６５２（以下「関連技術１」という。）及び特開２０００－１９４８３２（以下「関連技術２」という。）に開示されるものが挙げられる。

【０００４】関連技術１は、電子透かしが埋め込まれているデジタルコンテンツをプリンタで印刷する場合に、印刷データを適切に制御してデジタルコンテンツの著作権を保護することを課題とするものである。かかる課題を解決するための技術として、関連技術１は、電子透かしを抽出し画像の濃度値に埋め込み情報を加える等の変更処理を行い、画像を変形する技術を提案している。

【０００５】関連技術２は、図形や文字等のオブジェクトをデータとして保存する際、そのデータに対して付加情報を電子透かしによって埋め込むことによって、データの出力時にユーザから取得する付加情報が既に埋め込まれている付加情報と異なる場合にデータの出力を行えないようにする技術を提案している。

【０００６】また、本発明に関連する電子透かしの技術を用いた他の技術としては、特開平１１－２３９１２９（以下「関連技術３」という。）、特開２０００－２２７７５６（以下「関連技術４」という。）、及び特開２０００－２２７７５７（以下「関連技術５」という。）が挙げられる。これら関連技術３乃至５は、『電子データと個人／機関との関係をより高い信頼性をもって認証可能とすること、また電子データとの関係を認証可能な個人／機関と一致することが保証されるように電子データとの関係を持つ個人／機関を電子データによって利用者に直接提示すること』を課題としたものであり、その課題を解決するための手段として、『プロバイダー装置は購入者の公開鍵を用いて、購入者が購入したコンテンツを暗号化して送付する。購入者装置は自身の秘密鍵を用いてコンテンツの電子署名を作成し、作成した電子署名を電子透かしとして送付されたコンテンツに埋めこむ。不正コピーを入手した場合、プロバイダー装置は電子透かしの電子署名を検証し、この不正コピーの元となったコンテンツを購入した購入者を特定する』技術を提案したものである。

【０００７】更に、本発明に関連する他の技術として、特開平１１－１１９６５１（以下「関連技術６」という。）に開示されるものが挙げられる。この関連技術６においては、可視マークを消去し非可視マークを埋め込む際に可視マークの消去と非可視マークの埋め込みを不可分にすることを課題として可視マークの消去と非可視マークの埋め込みを並行して行う技術が示されている。

【０００８】

【発明が解決しようとする課題】しかしながら、上述した関連技術に見られるような手法では、コンテンツの著作権保護が適切になされない場合がある。

【０００９】例えば、上述した関連技術において、コンテンツに挿入される電子透かしは、大抵の場合、ユーザの入力した情報やユーザＩＤであり、ユーザが直接取り扱えるものである。従って、このユーザが悪意をもって第三者にそれらの情報やＩＤを知らせることも可能であり、それらの情報等を取得した第三者は、コンテンツの不正利用を行うことができる可能性がある。すなわち、上述した関連技術だけでは、コンテンツの不正利用を排除する効果が薄い。

【００１０】そこで、本発明は、上述した関連技術を踏まえた上で、より適切にコンテンツの著作権保護を図ることのできる手法及びそれを具現化する装置やシステムを提供することを目的とする。

【００１１】

【課題を解決するための手段】本発明の発明者は、上述した課題を解決するために検討を重ねた結果、デジタルコンテンツのある特性に着目した。

【００１２】すなわち、デジタルコンテンツは、オリジナルと同質のものを複製できるという特徴を有する一方、実体がデータであることから、何らかの出力装置に出力されて初めて、人間の認識することのできるものである。

【００１３】また、先に述べた「オリジナルと同質のものを複製できる」というデジタルコンテンツの特徴からも明らかなように、コンテンツの不正利用の形態において問題となるのは、例えば印刷された画像等そのものの授受よりも、コンテンツデータの授受である。そして、このような場合、コンテンツデータを不正に渡した者とそれを不正に受け取った者とは、それぞれ別個に、当該コンテンツデータを出力するための出力装置を所有していると考えられる。なお、ここでいう出力装置は、例えば、コンテンツデータが画像データの場合にあってはプリンタなどであり、他のデータにあってはそのデータを取り扱える装置を指す。

【００１４】これらのことから、本発明の発明者は、コンテンツデータを供給するにあたって、それを所望する

ユーザから当該ユーザの所有する出力装置のＩＤを取得し、そのＩＤを含むような電子透かし情報をコンテンツデータに埋め込むこととして、出力可能な出力装置を特定した状態でコンテンツデータを配信するというシステムを構築することが有効であると考えた。

【００１５】このようなシステムにおいては、例えばコンテンツデータが画像データであり出力装置がプリンタである場合を例にとると、画像データを正規に取得したユーザの所有するプリンタでしか、当該画像データで示される画像を印刷することができないこととなる。すなわち、画像データを第三者に不正に渡したとしても、第三者は、当該第三者の有するプリンタでは、その画像を印刷することができず、上述した関連技術よりも著作権保護を適切に図ることができる。しかも、このような概念は、出力装置がプリンタでない場合にも適用可能であり、画像データ以外のコンテンツデータに関しても、有効である。

【００１６】本発明は、具体的には、上述した課題を解決するための手段として、以下に示すコンテンツデータ供給方法を提供する。

【００１７】すなわち、本発明によれば、オリジナルコンテンツに係るオリジナルコンテンツデータを格納する第１のステップと、オリジナルコンテンツデータの供給を希望するユーザに対して、当該ユーザの所有する出力装置のＩＤの入力を促す第２のステップと、前記ユーザの所有する出力装置コントローラにより取り扱い可能な所定の電子透かし方法に従い、ユーザから入力された前記ＩＤを一部に含む電子透かし情報を前記オリジナルコンテンツデータに挿入して、マーク付コンテンツデータを生成する第３のステップと、前記ユーザに対して、前記マーク付コンテンツデータを供給する第４のステップとを含むことを特徴とするコンテンツデータ供給方法が得られる。

【００１８】ここで、前記第３のステップにおいて挿入される電子透かし情報を、前記オリジナルコンテンツ上に可視マークを形成するものであることとしても良い。

【００１９】また、前記オリジナルコンテンツデータは、画像データであることとしても良い。

【００２０】更に、前記出力装置としてプリンタを対象とし、前記オリジナルコンテンツデータとして印刷可能なデータを供給することとしても良い。

【００２１】また、前記第４のステップは、前記ユーザに対してネットワークを介して前記マーク付コンテンツデータを送信することにより、行われることとしても良く、前記ユーザの用意した蓄積媒体に対して前記マーク付コンテンツデータを蓄積することにより、行われることとしても良い。

【００２２】更に、上述したコンテンツデータ供給方法を次のように応用しても良い。

【００２３】すなわち、上述したコンテンツデータ供給方法において、前記ユーザとの間で電子署名を用いた認証処理を行い、該ユーザと共有する共通鍵を生成するステップを更に備え、前記第４のステップは、前記共通鍵により暗号化された前記マーク付コンテンツデータを供給するものであることとしても良い。

【００２４】また、上述したコンテンツデータ供給方法において、前記オリジナルコンテンツデータの利用料金を当該オリジナルコンテンツデータに関連付けて予め格納しておくステップと、前記ユーザの希望したオリジナルコンテンツデータに関連付けられた前記利用料金を取得するステップと、前記ユーザに対して当該取得した利用料金を通知するステップとを更に備えることとしても良い。

【００２５】また、本発明は、以下に列挙するように、上記したコンテンツデータ供給方法を実現するコンテンツデータ供給装置をも提供する。

【００２６】すなわち、本発明によれば、オリジナルコンテンツに係るオリジナルコンテンツデータを格納する格納部と、オリジナルコンテンツデータの供給を希望するユーザから当該ユーザの所有する出力装置のＩＤを取得するＩＤ取得部と、前記ユーザの所有する出力装置コントローラにより取り扱い可能な電子透かし方法に従い、前記取得したＩＤを一部に含む電子透かし情報を前記オリジナルコンテンツデータに挿入して、マーク付コンテンツデータを生成する電子透かし挿入部と、前記ユーザに対して、前記マーク付コンテンツデータを供給する供給部とを含むことを特徴とするコンテンツデータ供給装置が得られる。

【００２７】ここで、前記電子透かし挿入部において挿入される電子透かし情報を、前記オリジナルコンテンツ上に可視マークを形成するものであることとしても良い。

【００２８】また、前記ＩＤ取得部及び前記供給部は、前記ユーザの所有する出力装置コントローラの接続されたネットワークに対して、接続されており、前記ＩＤの取得及び前記マーク付コンテンツデータの供給は、前記ネットワークを介して行われることとしても良い。

【００２９】更には、前記ＩＤ取得部は、第１の種類の記録媒体に記録された情報を読取可能なものであり、前記ＩＤの取得は、予め前記ＩＤの格納された前記ユーザの所有する前記第１の種類の記録媒体から前記ＩＤを読み出すことにより行われ、前記供給部は、第２の種類の記録媒体に対して情報を書込み可能なものであり、前記マーク付コンテンツデータの供給は、前記ユーザの所有する前記第２の種類の記録媒体に対して前記マーク付コンテンツデータを書込むことにより行われることとしても良い。

【００３０】更に、上述したコンテンツデータ供給装置に対して次のように変形を加えても良い。

【００３１】すなわち、上述したコンテンツデータ供給

装置において、前記出力装置コントローラが電子認証を行うための第１の認証部を有するものである場合に、該第１の認証部との間で認証処理を行い、前記出力装置コントローラと共有する共通鍵の生成を行う第２の認証部と、該第２の認証部において生成された前記共通鍵を用いて、前記電子透かし挿入部において生成された前記マーク付コンテンツデータを暗号化する暗号化部とを更に備えており、前記供給部は、前記ユーザに対して、暗号化された前記マーク付コンテンツデータを供給することとしても良い。

【００３２】また、上述したコンテンツデータ供給装置において、前記格納部は、前記オリジナルコンテンツデータの利用料金を前記オリジナルコンテンツデータに関連付けて格納するものであり、その場合において、前記ユーザの希望したオリジナルコンテンツデータに関連付けられた前記利用料金を前記格納部から取得し、前記ユーザに対して取得した利用料金の通知を行う課金情報管理部を更に備えることとしても良い。

【００３３】更に、本発明は、上記したコンテンツデータ供給装置と共に、本発明によるシステムを構成し得る出力装置コントローラをも提供する。

【００３４】すなわち、本発明によれば、第１の出力装置コントローラとして、出力装置とコンテンツデータ供給装置とに接続された状態で使用される出力装置コントローラであって、前記出力装置は固有のＩＤを有するものであり、前記コンテンツデータ供給装置は所定の電子透かし方法に従ってオリジナルコンテンツデータに対し前記出力装置のＩＤを電子透かし情報の一部として挿入すると共に前記電子透かし情報の挿入されたオリジナルコンテンツデータをマーク付コンテンツデータとして出力するものである、出力装置コントローラにおいて、前記出力装置から前記ＩＤを取得し、前記コンテンツデータ供給装置に対して通知すると共に、当該取得したＩＤを保持するＩＤ取得部と、前記コンテンツデータ供給装置から前記マーク付コンテンツデータを取得するコンテンツ取得部と、取得したマーク付コンテンツデータから電子透かし情報を抽出する電子透かし抽出部と、抽出した電子透かし情報の一部と、前記ＩＤ取得部において保持されていたＩＤとを比較し、両者が同一であるか否かを判定するＩＤ判定部と、該ＩＤ判定部における判定の結果、両者が同一である場合に、前記マーク付コンテンツデータを変形して変形されたコンテンツデータを生成するコンテンツデータ変形部と、前記変形されたコンテンツデータから、前記出力装置において取扱可能な出力データを生成する出力データ生成部とを備えることを特徴とする出力装置コントローラが得られる。

【００３５】ここで、前記コンテンツデータ変形部における変形は、前記マーク付コンテンツデータから前記電子透かし情報を除去して前記オリジナルコンテンツデータを復元することである、こととしても良い。

【００３６】また、前記コンテンツデータ供給装置が電子認証を行うための第１の認証部を有するものであると共に前記マーク付コンテンツデータを所定の鍵で暗号化することのできるものである場合において、該第１の認証部との間で認証処理を行い、前記所定の鍵として、前記コンテンツデータ供給装置と共有する共通鍵の生成を行う第２の認証部と、前記コンテンツデータ供給装置において前記共通鍵を用いて暗号化された前記マーク付コンテンツデータから、前記マーク付コンテンツデータを復号化し、復号化した前記マーク付コンテンツデータを前記コンテンツ取得部に出力する復号部とを更に備えることとしても良い。

【００３７】更に、本発明によれば、第２の出力装置コントローラとして、出力装置とコンテンツデータ供給装置とに接続された状態で使用される出力装置コントローラであって、前記出力装置は固有のＩＤを有するものであり、前記コンテンツデータ供給装置は所定の電子透かし方法に従ってオリジナルコンテンツデータに対し前記出力装置のＩＤを一部に含む第１の電子透かし情報を挿入すると共に該第１の電子透かし情報の挿入されたオリジナルコンテンツデータを第１のマーク付コンテンツデータとして出力するものである、出力装置コントローラにおいて、前記出力装置から前記ＩＤを取得し、前記コンテンツデータ供給装置に対して通知すると共に、当該取得したＩＤを一時的に保持するＩＤ取得部と、前記コンテンツデータ供給装置から前記第１のマーク付コンテンツデータを取得するコンテンツ取得部と、取得した該第１のマーク付コンテンツデータから第１の電子透かし情報を抽出する電子透かし抽出部と、抽出した第１の電子透かし情報の一部に含まれるＩＤと、前記ＩＤ取得部において保持されていたＩＤとを比較し、両者が同一であるか否かを判定するＩＤ判定部と、該ＩＤ判定部における判定の結果、両者が同一である場合に、前記第１のマーク付コンテンツデータを変形して変形されたコンテンツデータを生成するコンテンツデータ変形部と、前記変形されたコンテンツデータに対して前記ＩＤ取得部において保持されていたＩＤを一部に含む第２の電子透かし情報の一部を挿入し、第２のマーク付コンテンツデータを生成するコントローラ側電子透かし挿入部と、該第２のマーク付コンテンツデータから、前記出力装置において取扱可能な出力データを生成する出力データ生成部とを備えることを特徴とする出力装置コントローラが得られる。

【００３８】ここで、前記コントローラ側電子透かし挿入部において挿入される第２の電子透かし情報は、前記コンテンツデータ変形部において生成された前記変形されたコンテンツデータの示すコンテンツ上に非可視マークを形成するものであることとしても良い。

【００３９】また、前記コンテンツデータ変形部における変形は、前記マーク付コンテンツデータから前記電子

透かし情報を除去して前記オリジナルコンテンツデータを復元することである、こととしても良い。

【００４０】更には、前記コンテンツデータ供給装置が電子認証を行うための第１の認証部を有するものであると共に前記マーク付コンテンツデータを所定の鍵で暗号化することのできるものである場合において、該第１の認証部との間で認証処理を行い、前記所定の鍵として、前記コンテンツデータ供給装置と共有する共通鍵の生成を行う第２の認証部と、前記コンテンツデータ供給装置において前記共通鍵を用いて暗号化された前記マーク付コンテンツデータから、前記マーク付コンテンツデータを復号化し、復号化した前記マーク付コンテンツデータを前記コンテンツ取得部に出力する復号部とを更に備えることとしても良い。

【００４１】

【発明の実施の形態】以下、本発明の実施の形態によるコンテンツデータ供給方法及びそれを具現化したコンテンツデータ供給システムについて、図面を用いて説明する。

【００４２】（第１の実施の形態）本発明の第１の実施の形態によるコンテンツデータ供給システムは、概略、図１に示されるように、出力装置コントローラ１０、出力装置２０、及びコンテンツデータ供給装置３０とを備えている。このうち、出力装置２０は、固有のＩＤを有しており、出力装置コントローラ１０と接続されている。また、出力装置コントローラ１０は、コンテンツデータ３０との間でデータの授受を行うことができる。

【００４３】ここで、各装置の詳細については、種々例を挙げながら後述することとし、まず、それらの概略について、図２を参照しながら、システムの概略動作説明と併せて言及する。なお、以下においては、出力装置２０としてプリンタを（従って、以下においては、「プリンタ」に参照符号２０を付す。）を例にとり説明するが、本発明の概念が他の出力装置に対しても同様に適用可能であることは言うまでもない。

【００４４】図２に示されるように、出力装置コントローラ１０は、プリンタ２０から当該プリンタ２０のＩＤを取得し、それをコンテンツデータ供給装置３０側に通知する。コンテンツデータ供給装置３０は、プリンタ２０及び出力装置コントローラ１０を所有するユーザの希望するコンテンツデータ（以下、変形等されるコンテンツデータと区別するために「オリジナルコンテンツデータ」という。）に対して、出力装置コントローラ１０から通知されたＩＤを含むような電子透かし情報を埋め込み、マーク付コンテンツデータとして、出力装置コントローラ２０に供給する。出力装置コントローラ１０は、マーク付コンテンツデータに挿入されている電子透かし情報の一部をなすＩＤと、プリンタ２０から取得したＩＤとが同一であるか否か判定し、両者が同一であった場合には、マーク付コンテンツデータの変形を行った上で、プリンタ２０にて印刷可能な印刷データを生成する。この印刷データは、出力装置コントローラ１０からプリンタ２０に対して出力され、プリンタ２０において印刷される。特に、本実施の形態においては、プリンタ２０は、自己調査を行い、印刷結果が正常に終了したか否かを印刷結果情報として、出力装置コントローラ１０に通知する。

【００４５】このような手法を採用することにより、コンテンツデータ供給装置側からすれば、印刷可能なプリンタを特定した状態でコンテンツデータの配信を行うことができる。また、ユーザ側においては、例えば第三者にコンテンツデータの複製を受渡すなどの不正利用を行おうとしても、ＩＤの一致したプリンタでしか正常に印刷し得ない、即ち、第三者の有するプリンタでは正常に印刷できないため、不正利用の抑制が図られる。

【００４６】ここで、出力装置２０と出力装置コントローラ１０とを接続する伝送路は、例えばＩＥＥＥ１３９４高速シリアルバス（ＩＥＥＥ Ｓｔｄ １３９４－１９９５，Ｓｔａｎｄａｒｄ ｆｏｒ ａ Ｈｉｇｈ Ｐｅｒｆｏｒｍａｎｃｅ Ｓｅｒｉａｌ Ｂｕｓ）やＵｎｉｖｅｒｓａｌ Ｓｅｒｉａｌ Ｂｕｓ（ＵＳＢ）などのシリアルインタフェースや、従来からパーソナルコンピュータ（以下「ＰＣ」と略す。）とプリンタを接続するために用いられていたパラレルインタフェースなどで構成することができる。

【００４７】また、図１に示されるように、出力装置コントローラ１０とコンテンツデータ供給装置３０との間のデータ授受手段としては、例えば、インターネットに代表されるネットワークなどや、蓄積媒体、放送媒体などを採用することができる。ネットワークをデータ授受手段として採用する場合にあっては、そのネットワークを構成する物理レベルについて、何らの制限もない。すなわち、電話線（アナログ加入者線）、ＩＳＤＮ、ｘＤＳＬ、ケーブルモデム、光ファイバなど、どのような通信媒体を用いても良い。また、蓄積媒体に関しても、特に制限はなく、ＦＤや、ＭＯ、ＣＤ－ＲＯＭ、ＤＶＤ、磁気テープなどのいずれを用いても良い。放送媒体についても、ＣＳデジタル放送やＢＳデジタル放送、地上波デジタル放送など、システム構成に応じて、種々採用可能である。

【００４８】データ授受手段がインターネットである場合には、例えば、コンテンツデータ供給装置３０をデータベース等と連携させたＷＷＷサーバなどで構成し、出力装置コントローラ１０をユーザサイドのＰＣ上で稼動するＷＷＷブラウザのプラグインとして構成することができる。この場合、コンテンツデータ供給装置３０は、種々の情報提供やＩＤ要求などのデータ入力要求はＷｅｂページ等の形態でユーザ側ＷＷＷブラウザに通知することができる。

【００４９】また、データ授受手段が蓄積媒体である場

合には、例えば、コンテンツデータ供給装置３０は、コンビニエンスストア等に設置されるキオスク端末として構成することができ、また、出力装置コントローラ１０は、ユーザの所有するＰＣ上で動作するプログラムとして構成することができる。この場合にあっては、コンテンツデータ供給の概略は、例えば、次のようなものとなる。まず、ユーザは、プリンタ２０の接続されたＰＣ上で出力装置コントローラを実現するプログラムを一旦実行して、プリンタのＩＤを蓄積媒体に格納した状態で、コンテンツデータ供給装置３０の設置されている場所まで出向く。コンテンツデータ供給装置３０にはユーザへの指示等を通知するためのパネルが設けられており、そこにＩＤを格納した蓄積媒体の挿入要求などが表示される。ユーザが、その要求に応じて蓄積媒体をコンテンツ供給装置３０に挿入して、コンテンツデータの指定を行うと、コンテンツデータ供給装置３０は、上述したようにして、電子透かし挿入を行い、マーク付コンテンツデータを蓄積媒体に書き込む。ユーザは、出力装置コントローラ１０をＰＣ上で再び実行し、蓄積媒体に記憶されたマーク付コンテンツデータを処理してプリンタ２０に印刷する。

【００５０】更に、コンテンツデータ供給装置３０をコンビニエンスストア等に設置されるキオスク端末として構成する場合にあっては、オリジナルコンテンツデータを格納する装置をセンターに置き、電子透かし挿入等を実行するその他の部分をキオスク端末に設けることとしても良い。更に、この場合にあっては、センターとキオスク端末との接続は、既存のネットワークを利用することとしても良い。

【００５１】なお、出力装置コントローラ１０とプリンタ２０との間でやりとりされるデータ及び出力装置コントローラ１０とコンテンツデータ供給装置３０との間で授受されるデータは、夫々、適切な暗号化処理を施されることが望ましい。例えば、後者に関連し、特にデータ授受手段がインターネットである場合、ＳＳＬ技術やＸＨＴＭＬなどを適用することが可能である。また、出力装置コントローラ１０、プリンタ２０及びコンテンツデータ供給装置３０の各装置内部で行われる処理がプロセッサとプログラムとの組み合わせにより達成される場合、ユーザにより、その処理内容が知られたり改竄されたりすることを防ぐために、タンパレジスタリング手法を用いて処理プログラムを難読化することが望ましい。

【００５２】以下、図３乃至図６を用いて、上述したコンテンツデータ供給システムに適用可能な出力装置コントローラ１０、プリンタ２０、及びコンテンツデータ供給装置３０について、より詳細に説明する。

【００５３】図３は、本実施の形態における出力装置コントローラ１０及びプリンタ２０の構成を示すブロック図である。

【００５４】図３を参照すると、出力装置コントローラ１０は、コンテンツ取得部１１０、電子透かし抽出部１２０、ＩＤ判定部１３０、コンテンツ変形部１４０、ＩＤ取得部１５０、及び印刷データ生成部１６０を備えている。一方、プリンタ２０は、自己のＩＤを格納するためのＩＤ格納部２１０、印刷データを印刷するための印刷部２２０を備えている。このうち、ＩＤ格納部２１０は、何らかのハードウェアに限定されるものではなく、例えば、ＲＯＭ、ＲＡＭなどの半導体メモリ、光磁気ディスクなどの磁気記録媒体、またこれらを含むＩＣカードや不揮発メモリカードなどで構成することができる。

【００５５】図示された出力装置コントローラ１０において、ＩＤ取得部１５０は、プリンタ２０のＩＤ格納部２１０からＩＤを取得し、そのＩＤを一時的に保持すると共に、コンテンツデータ供給装置３０に通知する。これにより、コンテンツデータ供給装置３０側においては、オリジナルコンテンツに対して、所定の電子透かし法に従って、通知されたＩＤを一部に含む電子透かし情報を挿入し、マーク付コンテンツデータとして出力装置コントローラ１０に供給することができる。コンテンツ取得部１１０は、コンテンツデータ供給装置３０から、マーク付コンテンツデータを取得する。電子透かし抽出部１２０は、マーク付コンテンツデータに埋め込まれている電子透かし情報を抽出する。ＩＤ判定部１３０は、ＩＤ取得部１５０に一時的に保持されているＩＤと電子透かし情報の一部をなすＩＤ（コンテンツデータ供給装置側において埋め込まれたＩＤ）とを比較し、両者が一致しているか否かを判定する。コンテンツ変形部１４０は、マーク付コンテンツデータの変形処理を行い、変形されたコンテンツデータを出力する。ここで、本実施の形態における変形処理は、ＩＤ判定部１３０において比較対象となるＩＤ同士が一致している場合において、マーク付コンテンツデータから電子透かしを除去し、オリジナルコンテンツデータを復元するものであるとする。印刷データ生成部１６０は、変形されたコンテンツデータ（すなわち、復元されたオリジナルコンテンツデータ）から、プリンタ２０にて取り扱い可能な印刷データを生成し、印刷部２２０に出力する。これにより、プリンタ２０においては、オリジナルコンテンツデータで示されるオリジナルコンテンツが印刷される。

【００５６】ここで、本実施の形態において用いられる電子透かし方式について説明する。本実施の形態において用いられる電子透かし方式は、その特徴として、電子透かし抽出部１２０において電子透かし情報が抽出できること、またコンテンツ変形部１４０において電子透かしの除去などの変形ができることを備えていればよい。したがって、ある特定の電子透かし方式に限定されるものではなく、例えば、中里、松井：“積極的に著作権を表示する署名透かし方式の提案”、画像電子学会誌第２７巻第５号（１９９８）で示されるような方式を用いることができる。この方式においてペアノ走査による署名

法と署名情報の分散秘匿化による電子透かしの二つの方法を同時に用いることが好適である。ベアノ走査による署名法においては、原画像に対して署名に用いる擬似乱数系列を用意し、ベアノ走査順に原画素と擬似乱数系列との排他的論理和をとることが特徴である。また、この他の電子透かし方式として、例えば、オリジナルコンテンツデータに対して高速フーリエ変換、離散コサイン変換、ウェーブレット変換などの周波数変換を行い、周波数領域に透かし情報を加えた後、逆周波数変換を行う方式を用いることができる。一例として前記高速フーリエ変換による電子透かし方式においては、オリジナルコンテンツデータはＰＮ系列を加えられて拡散された後、ブロック毎にフーリエ変換が行われ、さらに透かし情報が埋めこまれたブロックは逆フーリエ変換が行われた後、再び同じＰＮ系列が加えられて、電子透かしが埋めこまれればよい。

【００５７】また、電子透かし抽出部１２０においてマーク付コンテンツデータに埋め込まれている電子透かし情報を抽出する方法について言及すると、例えば図１に示されるデータ授受手段がインターネットなどである場合においては、インターネットを介して電子透かし情報を抽出する方法に関する情報を取得し、この情報に基づいて電子透かし情報を抽出する方法が好適である。

【００５８】更に、上述したように本実施の形態において、コンテンツ変形部１４０は、マーク付コンテンツデータの変形処理として、マーク付コンテンツデータから電子透かしを除去し、オリジナルコンテンツデータを復元することを行う。これに関し、より具体的には、例えば、コンテンツデータ供給装置３０において挿入される電子透かし情報が可視マークすなわち可視型の電子透かし方式で埋めこまれた電子透かし情報であるとし、コンテンツ変形部１４０は、この可視マークの消去を行うこととするのが好適である。

【００５９】また、印刷データ生成部１６０において、変形されたコンテンツデータからプリンタ２０が取り扱い可能な印刷データを生成する処理は、例えば誤差拡散手法などを用い、画像データを２値化しその２値化データをバンドメモリに展開する処理方法やまた画像データを多値データとしてバンドメモリに展開しこのデータをラスタライン単位で２値化する処理方法を用いることが好適である。

【００６０】図４は、本実施の形態における出力装置コントローラ１０ａの他の構成例を示すブロック図である。

【００６１】図４を参照すると、出力装置コントローラ１０ａは、コンテンツ取得部１１０、電子透かし抽出部１２０、ＩＤ判定部１３０、コンテンツ変形部１４０、ＩＤ取得部１５０、印刷データ生成部１６０、及び電子透かし挿入部１７０を備えている。このうち、コンテンツ取得部１１０、電子透かし抽出部１２０、ＩＤ判定部１３０、コンテンツ変形部１４０、及びＩＤ取得部１５０は、図３に示される出力装置コントローラ１０に含まれるものと同様にして動作する。また、印刷データ生成部１６０は、図４から明らかなように、処理対象がコンテンツ変形部１４０の出力ではなく、電子透かし挿入部１７０の出力である点を除き、図３に示されるものと同様にして動作する。従って、これらについては、上述した例と同様の参照符号を付してある。

【００６２】この例示された出力装置コントローラ１０ａは、電子透かし挿入部１７０を更に備えている点で、上述した出力装置コントローラ１０と異なる。この電子透かし挿入部１７０は、コンテンツ変形部１４０の出力する変形されたコンテンツデータに対して、例えば、ＩＤ取得部１５０に保持されているＩＤを一部に含むような電子透かし情報を埋め込むためのものである。詳しくは、電子透かし挿入部１７０は、印刷を行うユーザの識別情報や出力装置コントローラ１０の識別情報若しくはプリンタ２０のＩＤなど印刷行為者や印刷制御システムに関する識別情報、及び／又は印刷行為を行う年月日や時刻などの時間情報などの情報を電子透かしとして、変形されたコンテンツデータに対して挿入するためのものである。

【００６３】ここで、電子透かし挿入部１７０において埋めこまれる透かし情報は非可視マークとすることが好適である。また、この場合、コンテンツデータ供給装置３０において埋めこまれる透かし情報は可視マークとすることが望ましい。更に、電子透かし方式として、例えば、可視マークを消去し非可視マークを埋めこむ際に可視マークの消去と非可視マークの埋め込みを並行して行う方式（特開平１１－１１９６５１）を用いることもできる。

【００６４】出力装置コントローラ１０ａをこのような構成とすることにより、例えば、仮に、コンテンツデータの不正利用が生じた場合にあっても、それに関与したユーザを特定し易くなる。

【００６５】ここで、出力装置コントローラ１０ａにおける動作について再度説明すると、まず、図示された出力装置コントローラ１０において、ＩＤ取得部１５０は、プリンタ２０のＩＤ格納部２１０からＩＤを取得し、そのＩＤを一時的に保持すると共に、コンテンツデータ供給装置３０に通知する。これにより、コンテンツデータ供給装置３０側においては、オリジナルコンテンツに対して、所定の電子透かし法に従って、通知されたＩＤを一部に含む電子透かし情報を挿入し、マーク付コンテンツデータとして出力装置コントローラ１０に供給することができる。コンテンツ取得部１１０は、コンテンツデータ供給装置３０から、マーク付コンテンツデータを取得する。電子透かし抽出部１２０は、マーク付コンテンツデータに埋め込まれている電子透かし情報を抽出する。ＩＤ判定部１３０は、ＩＤ取得部１５０に一時

的に保持されているＩＤと電子透かし情報の一部をなすＩＤ（コンテンツデータ供給装置側において埋め込まれたＩＤ）とを比較し、両者が一致しているか否かを判定する。コンテンツ変形部１４０は、マーク付コンテンツデータの変形処理を行い、変形されたコンテンツデータを出力する。ここで、本実施の形態における変形処理は、上述したように、マーク付コンテンツデータから電子透かしを除去し、オリジナルコンテンツデータを復元するものである。電子透かし挿入部１７０は、変形処理を施された後のコンテンツデータ（即ち、本実施の形態においては、復元されたオリジナルコンテンツデータ）に対して電子透かしの挿入処理を行う。印刷データ生成部１６０は、電子透かし挿入部１７０において電子透かしの挿入されたコンテンツデータから、プリンタ２０にて取り扱い可能な印刷データを生成し、印刷部２２０に出力する。ここで、電子透かし挿入部１７０において挿入される電子透かしが非可視マークである場合、印刷データは、オリジナルコンテンツを印刷した場合と同様の印刷結果を呈するものとなる。このような印刷データを受けて、プリンタ２０は、オリジナルコンテンツデータで示されるオリジナルコンテンツを印刷する。

【００６６】次に、図５を参照して、コンテンツデータ供給装置３０の具体的構成について、説明する。

【００６７】図５に示されるように、コンテンツデータ供給装置３０は、コンテンツ格納部３１０、電子透かし挿入部３２０、供給部３３０、ＩＤ取得部３４０を備えている。コンテンツ格納部３１０は、予め、オリジナルコンテンツデータを格納している。ＩＤ取得部３４０は、出力装置コントローラ１０から、インターネット等のデータ授受手段を介して、プリンタ２０のＩＤを取得する。具体的には、ＩＤ取得部３４０は、ユーザ側の出力装置コントローラ１０へ対して、ＩＤ送出要求等を送るなどして、ＩＤの入力を促し、それにより送出等されてきたＩＤを取得する。この際、これに先立って、又は、このＩＤ送出要求の直後に、ユーザ側からは、所望とするオリジナルコンテンツデータの指定を受付けておく。電子透かし挿入部３２０は、ＩＤ取得部３４０からＩＤを受け取ると、コンテンツ格納部３１０からユーザの所望するオリジナルコンテンツデータを取得し、そのオリジナルコンテンツデータに対して、所定の電子透かし挿入方法に従い、取得したＩＤを電子透かし情報として埋めこむ。ここで用いる所定の電子透かし挿入方法は、上述したような電子透かし方式によるものであり、電子透かし抽出部１２０において用いる電子透かし方式と同一のものであればよい。更に、電子透かし挿入部３２０は、そのような電子透かし情報の埋め込まれたオリジナルコンテンツデータを、マーク付コンテンツデータとして、供給部３３０に対して、出力する。供給部３３０は、インターネット等のデータ授受手段を介して、マーク付コンテンツデータを出力装置コントローラ１０に供給する。

【００６８】このコンテンツデータ供給装置３０におけるＩＤ取得部３４０及び供給部３３０は、データ授受手段がインターネット等のネットワークである場合、双方とも、そのネットワークに接続され、ネットワークを介してＩＤを取得し、又、ネットワークを介してマーク付コンテンツデータを供給する。一方、データ授受手段が蓄積媒体である場合、ＩＤ取得部３４０は、蓄積媒体に格納されたＩＤを読み込み、供給部３３０は、マーク付コンテンツデータを蓄積媒体に書込む。ここで、ＩＤの格納された蓄積媒体と、マーク付コンテンツデータの書込まれる蓄積媒体とは、同一メディアであっても良いし、異なるメディアであっても良い。

【００６９】コンテンツデータ供給装置は、キオスク端末的な使用形態でも使用可能であることは既に述べた通りであるが、そのうち、例えばコンビニエンスストア等に設置される場合であって、センターとネットワークで接続されるような形態にて用いられる場合には、図６に示されるように変形することも可能である。

【００７０】即ち、図６に示されるコンテンツデータ供給装置３０ａは、図５に示されるコンテンツデータ供給装置３０のうち、電子透かし挿入部３２０、供給部３３０及びＩＤ取得部３４０を備えている。一方、コンテンツデータ供給装置３０ａにネットワークで接続されるセンター側にはコンテンツ格納装置３１０ａが設けられる。このコンテンツ格納装置３１０ａは、図５に示されるコンテンツ格納部３１０と同様に、オリジナルコンテンツデータを格納するものであり、例えばデータベースで構成される。

【００７１】（第２の実施の形態）本発明の第２の実施の形態によるコンテンツデータ供給システムについて、図７乃至図９を用いて説明する。

【００７２】本実施の形態においては、コンテンツデータ供給装置３０は、図７に示されるように、上述した第１の実施の形態による構成（図５参照）に加え、認証部３５０、復号化部３６０及び暗号化部３７０を備えており、出力装置コントローラ１０もまた、図８に示されるように、上述した第１の実施の形態による構成（図３参照）に加え、認証部１８０、暗号化部１８２及び復号化部１８４を備えている。

【００７３】コンテンツデータ供給装置における認証部３５０と出力装置コントローラにおける認証部１８０とは、インターネット等のデータ授受手段を介して、所定の通信プロトコルに従った電子認証を行う。この電子認証は、電子署名および鍵配送方式により行うことが好適である。電子署名方式および鍵配送方式としては、これまで考案されている様々な方式を用いることが可能であり、例えば、楕円ＤＳＡ（Ｄｉｇｉｔａｌ　Ｓｉｇｎａｔｕｒｅ　Ａｌｇｏｒｉｔｈｍ）署名および楕円ＤＨ（Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎ）鍵配送を用いること

ができる。楕円ＤＳＡ署名（以下ＥＣ－ＤＳＡという）について以下に述べる。ＥＣ－ＤＳＡはＡＮＳＩ　Ｘ９．６２などに規定されており、その内容は、鍵生成、署名生成、署名照合の三つの段階からなる。なお、以下に、これらの各段階における手順を説明するが、重複する記載を省略するため、コンテンツデータ供給装置及び出力装置コントローラに代えて、デバイスＡ及びＢというように抽象化して説明する。換言すると、コンテンツデータ供給装置側の認証部３５０は、その主導により、電子認証を行う場合にあっては、デバイスＡとして動作し、受け手側として動作する場合にあっては、デバイスＢとして動作する。一方、出力装置コントローラも、同様である。

【００７４】まず、鍵生成の手順について説明する。

（１）　ＥＣ－ＤＳＡ鍵生成

デバイスＡにおいて：

ステップ１：　ＺＰ上に構成する楕円曲線Ｅを選択する。Ｅ（ＺＰ）上の点の数は大きな素数ｎで割り切れること。

ステップ２：　位数ｎの点Ｐ∈Ｅ（ＺＰ）を選択する。

ステップ３：　区間　［１，ｎ－１］のなかから静的に特有かつ予言できない整数ｄを選択する。

ステップ４：　Ｑ＝ｄＰを計算する。

ステップ５：　Ａの公開鍵は（Ｅ，Ｐ，ｎ，Ｑ）、Ａの秘密鍵はｄとする。

【００７５】つぎに、署名生成手順について説明する。

（２）　ＥＣ－ＤＳＡ署名生成

デバイスＡにおいて、以下のようにメッセージｍを暗号化する。

ステップ１：　区間　［１，ｎ－１］のなかから静的に特有かつ予言できない整数ｋを選択する。

ステップ２：　ｋＰ＝（ｘ１，ｙ１）およびｒ＝ｘ１　ｍｏｄ　ｎを計算する。ここでｘ１はたとえばバイナリ表現からの変換によって一つの整数と見なされる。もしｒ＝０ならばステップ１に戻る（セキュリティ上の理由。ｒ＝０なら暗号等式　ｓ＝ｋ－１｛ｈ（ｍ）＋ｄｒ｝　ｍｏｄ　ｎ　が秘密鍵ｄを含まないため）。

ステップ３：　ｋ－１　ｍｏｄ　ｎ　を計算する。

ステップ４：　ｓ＝ｋ－１｛ｈ（ｍ）＋ｄｒ｝　ｍｏｄ　ｎを計算する。ここでｈはセキュアハッシュアルゴリズム（ＳＨＡ－１）である。

ステップ５：　もしｓ＝０ならばステップ１に戻る（もしｓ＝０ならば、ｓ－１　ｍｏｄ　ｎが存在しない；ｓ－１は署名照合のステップ２で必要）。

ステップ６：　メッセージｍの署名を整数の組み（ｒ，ｓ）とする。

【００７６】続いて、署名照合の手順について説明する。

（３）　ＥＣ－ＤＳＡ署名照合

ｍのなかのデバイスＡの署名（ｒ，ｓ）を照合するために、デバイスＢは以下のことを行う。

ステップ１：　Ａの公開鍵（Ｅ，Ｐ，ｎ，Ｑ）の真のコピーを得る。

ステップ２：　ｒおよびｓが区間　［１，ｎ－１］　の整数であることを照合する。

ステップ３：　ｗ＝ｓ－１　ｍｏｄ　ｎおよびｈ（ｍ）を計算する。

ステップ４：　ｕ１＝ｈ（ｍ）ｗ　ｍｏｄ　ｎおよびｕ２＝ｒｗ　ｍｏｄ　ｎを計算する。

ステップ５：　ｕ１Ｐ＋ｕ２Ｑ＝（ｘ０，ｙ０）およびｖ＝ｘ０　ｍｏｄ　ｎを計算する。

ステップ６：　ｖ＝ｒならば署名を認める。

【００７７】次に、楕円ＤＨ鍵配送（以下ＥＣ－ＤＨという）について述べる。ＥＣ－ＤＨはＡＮＳＩ　Ｘ９．６３などに規定されており、その内容は鍵生成および交換と鍵共有の二つの段階からなる。まず、鍵生成および交換の手順は以下の通りである。

【００７８】（１）　ＥＣ－ＤＨ鍵生成および交換

デバイスＡにおいて

ステップ１：　区間　［２，ｎ－２］のなかから静的に特有かつ予言できない整数ｘを選択する。

ステップ２：　ａ＝ｘＰを計算する。

ステップ３：　デバイスＡはデバイスＢにａを送る。

デバイスＢにおいて

ステップ１：　区間　［２，ｎ－２］のなかから静的に特有かつ予言できない整数ｙを選択する。

ステップ２：　ｂ＝ｙＰを計算する。デバイスＢはデバイスＡにｂを送る。

【００７９】次に、鍵共有の手順を以下に述べる。

（２）　ＥＣ－ＤＨ鍵共有

ステップ１：　デバイスＡにおいてＫＡ＝ｘｂ＝ｘｙＰにより共通鍵を生成する。

ステップ２：　デバイスＢにおいてＫＢ＝ｘａ＝ｘｙＰにより共通鍵を生成する。

ステップ３：　ＫＡ＝ＫＢなのでデバイスＡとデバイスＢは鍵を共有する。

以上のような手順によって認証処理が行われる。

【００８０】このようにして共通鍵の共有がなされると、コンテンツデータ供給装置及び出力装置コントローラのそれぞれにおいて、この共通鍵を用いて暗号化及び復号化処理が行われ、その暗号化及び復号化処理を利用したコンテンツデータの供給が行われる。なお、暗号および復号の方式はこれまでに提案されているどのような方式でも用いることができる。

【００８１】以下、図９をも参照して、各部の動作及び機能について併せて説明する。まず、プリンタ２０は、ＩＤ格納部２１０に格納してある自身のＩＤを出力装置コントローラ１０に通知する（ＩＤ通知）。出力装置コントローラ１０は、認証部１８０を用いて電子署名を作成し、コンテンツデータ供給装置３０に送信し、一方、

コンテンツデータ供給装置３０は、認証部３５０を用いて電子署名を作成し、出力装置コントローラ１０に送信する（電子署名）。

【００８２】この電子認証処理の結果、出力装置コントローラ１０及びコンテンツデータ供給装置３０は、上述したように、共通鍵を共有することとなる。

【００８３】続いて、認証部１８０は、認証処理の結果得られた共通鍵を暗号化部１８２及び復号化部１８４に通知する。一方、コンテンツデータ供給装置側において、認証部３５０は、認証処理の結果得られた共通鍵を復号化部３６０及び暗号化部３７０に通知する。

【００８４】その上で、出力装置コントローラ側の暗号化部１８２は、ＩＤ取得部１５０からＩＤを受けると、その共通鍵を用いて、暗号化処理を行い、コンテンツデータ供給装置側に暗号化されたＩＤを送出する（暗号化ＩＤ通知）。

【００８５】コンテンツデータ供給装置側の復号化部３６０は、暗号化されたＩＤを受けると、共通鍵を用いて、復号化処理を行い、復号化したＩＤをＩＤ取得部３４０に通知する。その後、供給部３３０からマーク付コンテンツデータが出力されるまでは、上述した第１の実施の形態と同じである。

【００８６】コンテンツデータ供給装置側の暗号化部３７０は、供給部３３０からマーク付コンテンツデータを受けると、共通鍵を用いて、暗号化処理を行い、暗号化したマーク付コンテンツデータを出力装置コントローラ側に供給する（暗号化コンテンツ供給）。

【００８７】出力装置コントローラ側の復号化部１８４は、コンテンツデータ供給装置側から暗号化されたマーク付コンテンツデータを受け取ると、認証部１８０から受けた共通鍵を用いて復号化処理を行い、復号化されたマーク付コンテンツデータをコンテンツ取得部１１０に出力する。その後、印刷データ生成部１６０から印刷データが出力され、プリンタ２０において印刷されるまでの過程は、上述した第１の実施の形態と同様にして行われる。また、本実施の形態においても、第１の実施の形態と同様、プリンタ２０は、自己調査を行い、印刷結果が正常に終了したか否かを印刷結果情報として、出力装置コントローラ１０に通知する。

【００８８】なお、本実施の形態においても、各装置内部で行われる処理に関して、ユーザにより、その処理内容が知られたり改竄されたりすることを防ぐために、タンパレジスタリング手法を用いて処理プログラムを難読化することが望ましい。

【００８９】上述した第２の実施の形態においては、図７及び図８に示されるように、コンテンツデータ供給装置３０及び出力装置コントローラ１０の双方とも暗号化部（３７０及び１８２）及び復号化部（３６０及び１８４）を備える構成を示したが、コンテンツデータ供給装置３０が復号化部３６０を備え且つ暗号化部３７０を備えないこととし、一方、出力装置コントローラ１０が暗号化部１８２を備え且つ復号化部１８４を備えない構成としても良いし、その逆としても良い。更に、プリンタ２０にも認証部と復号化部を備えて構成することも可能である。

【００９０】また、上述した実施の形態においては、図３及び図５に示される出力装置コントローラ１０及びコンテンツデータ供給装置３０をベースとして認証部、暗号化部及び復号化部を備えるように変形した例を用いて説明してきたが、出力装置コントローラに関して言えば、図４に示されるものをベースとしても良く、また、コンテンツデータ供給装置に関して言えば、図６に示されるものをベースとしても良い。

【００９１】（第３の実施の形態）本発明の第３の実施の形態によるコンテンツデータ供給システムについて、図１０乃至図１２を用いて説明する。

【００９２】本実施の形態におけるコンテンツデータ供給装置は、図１０に示されるように、上述した第１の実施の形態による構成（図５参照）に加え、課金情報管理部３８０を有している。課金情報管理部３８０は、オリジナルコンテンツデータに関連付けられた利用料金等の課金情報を格納してなるデータベースを有しており、コンテンツ格納部３１０から読み出されるオリジナルコンテンツデータに応じた課金情報を出力装置コントローラ側に送出するものである。ここで、課金情報を格納してなるデータベースは、課金情報管理部３８０と別個に設けても良いし、コンテンツ格納部３１０に組み込まれていても良い。また、図示された例においては、課金情報管理部３８０をコンテンツデータ供給装置に組み込んだ構成としているが、これをコンテンツデータ供給装置とは別個に設けることとしてもよい。その場合にあっても、利用料金等の課金情報を格納してなるデータベースについては、独立した課金情報管理部に組み込まれていても良いし、それ自身独立するように設けられていても良いし、また、コンテンツ格納部３１０に組み込まれていても良い。

【００９３】なお、図１０に示される他の構成要素、すなわち、コンテンツ格納部３１０、電子透かし挿入部３２０、供給部３２０及びＩＤ取得部３４０は、上述した第１の実施の形態と同様にして動作する。

【００９４】一方、本実施の形態における出力装置コントローラは、図１１に示されるように、上述した第１の実施の形態による構成（図３参照）に加え、課金情報取得部１９０、課金料算出部１９２及び電子決済部１９４を備えている。課金情報取得部１９０は、課金管理格納部３８０から課金情報を取得するものである。課金料算出部１９２は、課金情報取得部１９０の取得した課金情報に基づいて、所定期間毎に、課金情報を集計し課金料を算出するものである。電子決済部４４０は、課金料算出部１９２の算出した課金料金を電子的に決済するため

のものであり、決済情報をコンテンツデータ供給装置（具体的には、課金情報管理部）に通知する。電子決済部４４０における電子決済手法としては、クレジットカードや電子マネーなどの既存の電子決済手法を採用することができる。なお、図１１においては、課金情報取得部１９０、課金料算出部１９２及び電子決済部１９４を出力装置コントローラに組み込んだ構成としているが、これらを出力装置コントローラと別個に設けることとしても良い。

【００９５】なお、図１１に示される他の構成要素、すなわち、コンテンツ取得部１１０、電子透かし抽出部１２０、ＩＤ判定部１３０、コンテンツ変形部１４０、ＩＤ取得部１５０及び印刷データ生成部１６０は、上述した第１の実施の形態と同様にして動作する。

【００９６】以下、図１２をも参照して、各部の動作について説明する。まず、プリンタ２０は、ＩＤ格納部２１０に格納してある自身のＩＤを出力装置コントローラ１０に通知する（ＩＤ通知）。出力装置コントローラ１０は、このＩＤをさらにコンテンツデータ供給装置３０に通知する（ＩＤ通知）。コンテンツデータ供給装置３０は、このＩＤを電子透かし情報の一部としてオリジナルコンテンツデータに埋め込み（電子透かし挿入）、マーク付コンテンツデータとして出力装置コントローラ１０に供給する（コンテンツ供給）。

【００９７】特に、本実施の形態においては、コンテンツデータ供給装置３０（具体的には、課金情報管理部）は、データベースの検索結果に従い、供給したコンテンツデータに対応する課金情報を出力装置コントローラ１０側に通知する（課金情報通知）。

【００９８】出力装置コントローラ１０は、マーク付コンテンツデータを受けると、ＩＤ判定、コンテンツ変形、印刷データの生成等を行い、印刷データをプリンタ２０に出力する（印刷データ出力）。プリンタ２０は、印刷データを用いて印刷を行い、正常に印刷できたか否かを示す印刷結果を出力装置コントローラ１０に対して通知する（印刷結果通知）。

【００９９】なお、図１２においては、課金情報通知が行われた後、出力装置コントローラ１０におけるＩＤ判定等の処理が行われるように示されているが、これらの処理は、いずれが先に行われても良い。

【０１００】出力装置コントローラにおいては、課金情報取得部１９０、課金料算出部１９２、電子決済部１９４によって、課金情報の取得、所定期間毎の課金情報の集計、電子決済の各処理が実行され、最終的に得られた決済情報がコンテンツデータ供給装置３０側の課金情報管理部３８０に通知される（決済情報通知）。

【０１０１】ここで、本実施の形態においても、前述の他の実施の形態と同様に、各装置間で授受される情報は、適切な暗号化処理を施されることが望ましく、また、各装置内部で行われる処理に関して、利用者にその処理内容が知られたり改竄されたりすることを防ぐために、タンパレジスタリング手法を用いて処理プログラムを難読化することが望ましい。

【０１０２】なお、上述した第３の実施の形態においては、図３及び図５に示される出力装置コントローラ１０及びコンテンツデータ供給装置３０をベースとして課金情報管理部３８０、課金情報取得部１９０、課金料算出部１９２、及び電子決済部１９４を備えるように変形した例を用いて説明してきたが、出力装置コントローラに関して言えば、図４に示されるものをベースとしても良く、また、コンテンツデータ供給装置に関して言えば、図６に示されるものをベースとしても良い。

【０１０３】

【発明の効果】以上説明したように、本発明のコンテンツデータ供給方法及びシステムによれば、コンテンツデータの供給時に、コンテンツデータを正常に出力可能な出力装置を特定した状態で供給できることから、コンテンツの著作権保護がより適切になされ得ることとなる。

【図面の簡単な説明】

【図１】本発明の実施の形態によるコンテンツデータ供給システムの概略構成を示す図である。

【図２】本発明の第１の実施の形態によるコンテンツデータ供給システムの概略動作を示す図である。

【図３】本発明の第１の実施の形態によるコンテンツデータ供給システムに適用可能な出力装置コントローラ及びプリンタの一例を示す図である。

【図４】本発明の第１の実施の形態によるコンテンツデータ供給システムに適用可能な出力装置コントローラ及びプリンタの他の例を示す図である。

【図５】本発明の第１の実施の形態によるコンテンツデータ供給システムに適用可能なコンテンツデータ供給装置の一例を示す図である。

【図６】本発明の第１の実施の形態によるコンテンツデータ供給システムに適用可能なコンテンツデータ供給装置の他の例を示す図である。

【図７】本発明の第２の実施の形態によるコンテンツデータ供給システムに適用可能な出力装置コントローラの一例を示す図である。

【図８】本発明の第２の実施の形態によるコンテンツデータ供給システムに適用可能なコンテンツデータ供給装置の一例を示す図である。

【図９】本発明の第２の実施の形態によるコンテンツデータ供給システムの概略動作を示す図である。

【図１０】本発明の第３の実施の形態によるコンテンツデータ供給システムに適用可能なコンテンツデータ供給装置の一例を示す図である。

【図１１】本発明の第３の実施の形態によるコンテンツデータ供給システムに適用可能な出力装置コントローラの一例を示す図である。

【図１２】本発明の第３の実施の形態によるコンテンツ

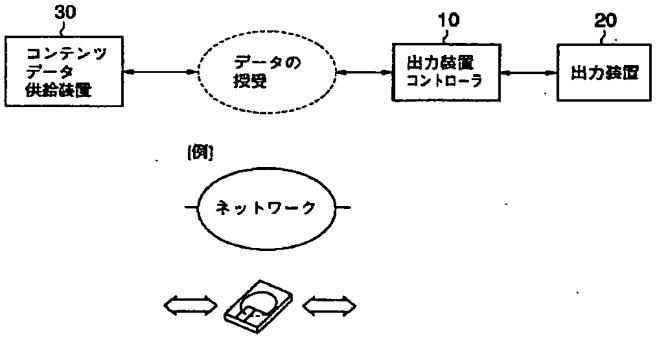
25　　26

データ供給システムの概略動作を示す図である。

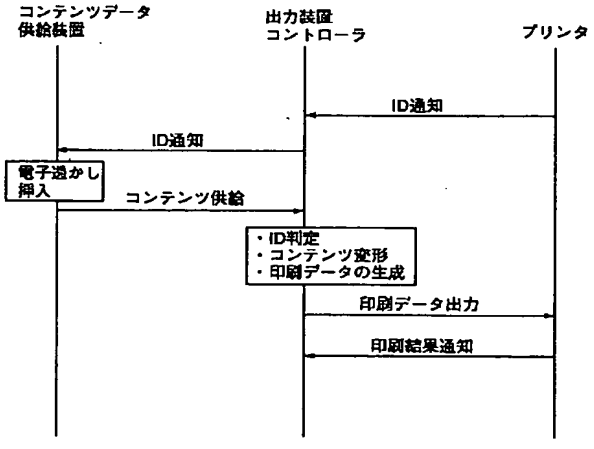
【符号の説明】

１０	出力装置コントローラ		＊１９２	課金料算出部
１１０	コンテンツ取得部		１９４	電子決済部
１２０	電子透かし抽出部		２０	出力装置（プリンタ）
１３０	ＩＤ判定部		２１０	ＩＤ格納部
１４０	コンテンツ変形部		２２０	印刷部
１５０	ＩＤ取得部		３０	コンテンツデータ供給装置
１６０	印刷データ生成部		３１０	コンテンツ格納部
１７０	電子透かし挿入部		３２０	電子透かし挿入部
１８０	認証部		３３０	供給部
１８２	暗号化部	10	３４０	ＩＤ取得部
１８４	復号化部		３５０	認証部
１９０	課金情報取得部		３６０	復号化部
			３７０	暗号化部
		＊	３８０	課金情報管理部

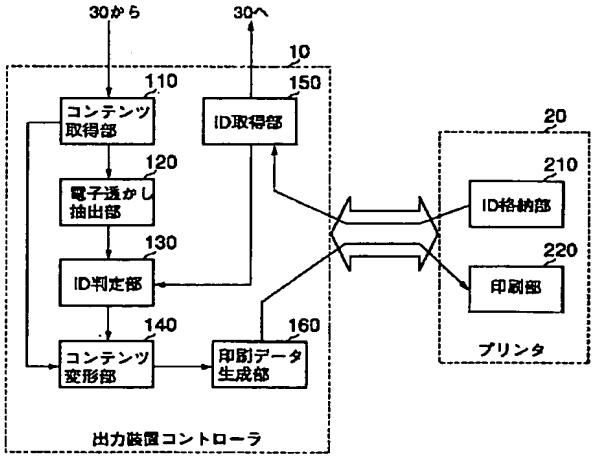
【図１】



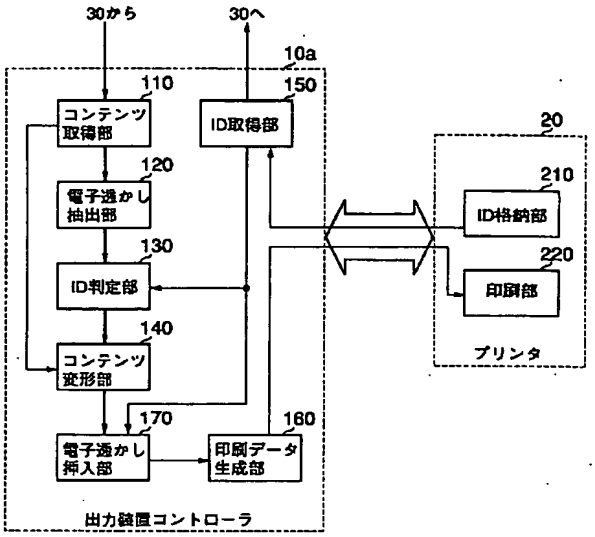
【図２】



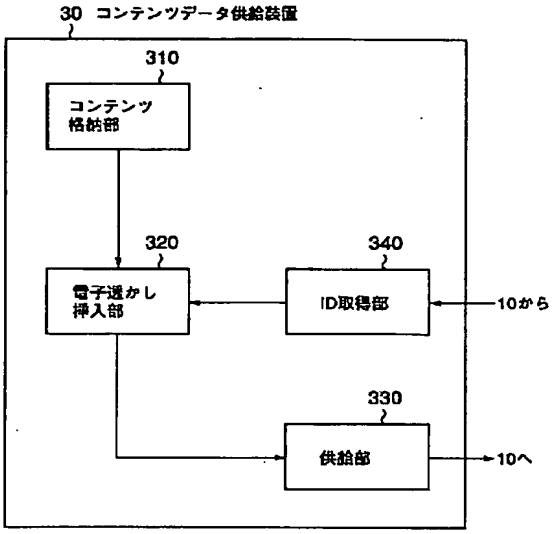
【図３】



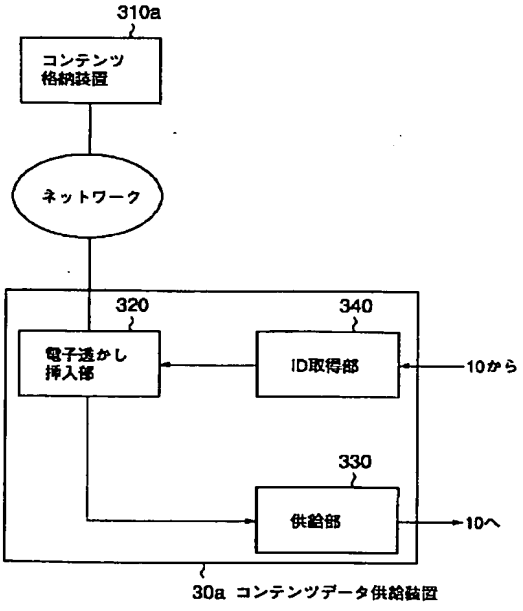
【図４】


30から
30へ
10a
110
コンテンツ取得部
150
ID取得部
20
120
電子透かし抽出部
210
ID格納部
130
ID判定部
220
印刷部
140
コンテンツ変形部
プリンタ
170
電子透かし挿入部
160
印刷データ生成部
出力装置コントローラ

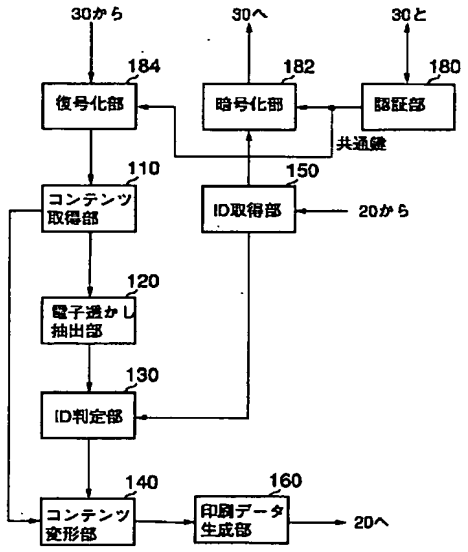
【図５】


30 コンテンツデータ供給装置
310
コンテンツ格納部
320
340
電子透かし挿入部
ID取得部
10から
330
供給部
10へ

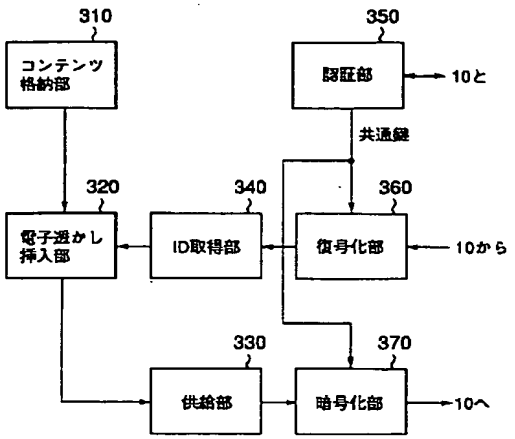
【図６】


310a
コンテンツ格納装置
ネットワーク
320
340
電子透かし挿入部
ID取得部
10から
330
供給部
10へ
30a コンテンツデータ供給装置

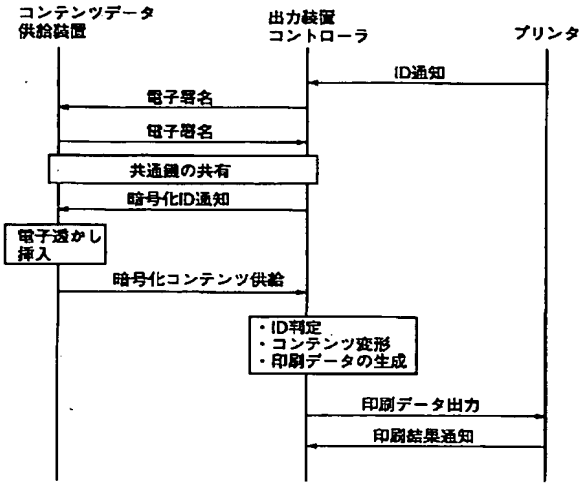
【図７】


30から
30へ
30と
184
182
180
復号化部
暗号化部
認証部
共通鍵
110
150
コンテンツ取得部
ID取得部
20から
120
電子透かし抽出部
130
ID判定部
140
160
コンテンツ変形部
印刷データ生成部
20へ

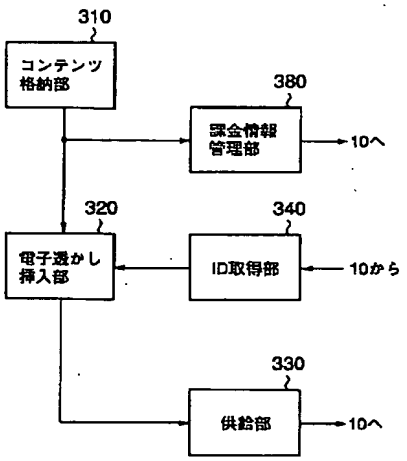
【図８】


310
コンテンツ格納部
350
認証部
10と
共通鍵
320
340
360
電子透かし挿入部
ID取得部
復号化部
10から
330
370
供給部
暗号化部
10へ

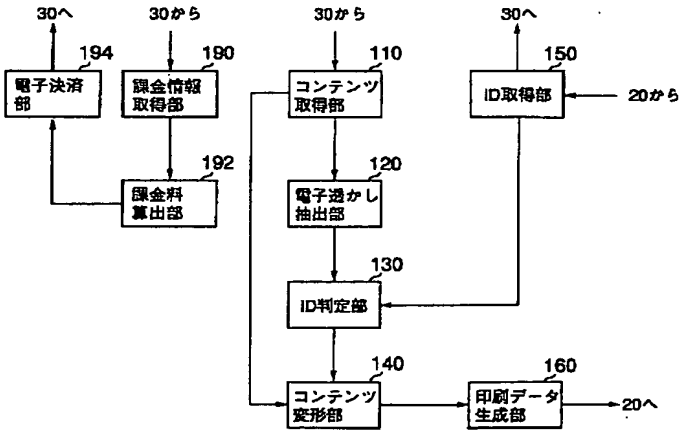
【図９】


コンテンツデータ供給装置
出力装置コントローラ
プリンタ
ID通知
電子署名
電子署名
共通鍵の共有
暗号化ID通知
電子透かし挿入
暗号化コンテンツ供給
・ID判定
・コンテンツ変形
・印刷データの生成
印刷データ出力
印刷結果通知

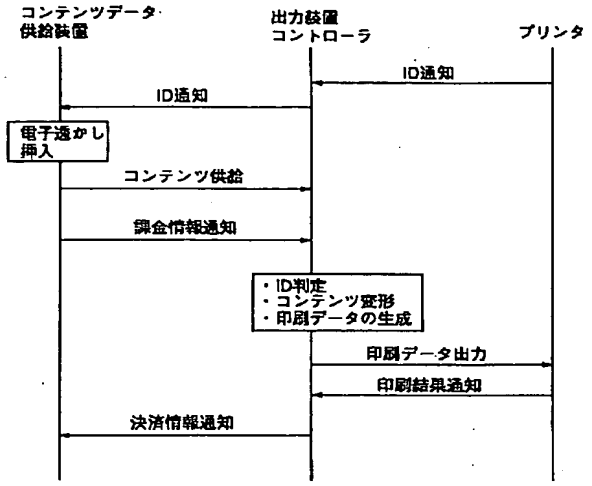
【図１０】


310
コンテンツ格納部
380
課金情報管理部
10へ
320
340
電子透かし挿入部
ID取得部
10から
330
供給部
10へ

【図１１】


30へ
30から
30から
30へ
194
190
110
150
電子決済部
課金情報取得部
コンテンツ取得部
ID取得部
20から
192
120
課金料算出部
電子透かし抽出部
130
ID判定部
140
160
コンテンツ変形部
印刷データ生成部
20へ

【図１２】



フロントページの続き

(51)Int.Cl.'	識別記号	FI	テーマコード(参考)
Ｈ０４Ｎ　7/173	６２０	Ｈ０４Ｎ　7/173	６４０Ａ　５Ｃ０６４
	６４０	Ｂ４１Ｊ　29/00	Ｚ　５Ｃ０７６

Ｆターム(参考)　2C061 AP01 BB17 CL10
2C087 AA13 BA03 BA04 BA05 BD12
DA13
2C187 GD01
5B057 AA11 CA08 CA12 CA16 CB08
CB12 CB16 CE08 CG05 CH08
5C052 AA11 DD02 FA02 FA03 FA07
FB01 FB05 FC04
5C064 BA02 BB02 BC07 BC20 BC25
BD03 BD09
5C076 AA14 BA03 BA05 BA06